# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 6, Task ID: 18

Task ID: 18 Risk Level:

Date Processed: 2016-04-08 09:39:50 (UTC)

Processing Time: 62.01 seconds

Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\ToggleService32.exe"

Sample ID: Type: basic Owner: admin

ToggleService32.exe Label: Date Added: 2016-04-08 09:39:50 (UTC)

File Type: PE32:win32 File Size: 10254 bytes

1439e0552127dda0c66b7be1eadb723d MD5:

SHA256: 89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a

Description:

### Pattern Matching Results

Modifies registry autorun entries

Writes to system32 folder

2 PE: Nonstandard section

5 Installs service

2 Resolves local hostname

6 PE: File has TLS callbacks Writes to a log file [Info]

4 Terminates process under Windows subfolder

4 Reads process memory

4 Connects to local IP

Injects thread into Windows process

### Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

PE: File contain TLS callbacks Anomaly:

#### Process/Thread Events

Creates process: C:\windows\temp\ToggleService32.exe

["C:\windows\temp\ToggleService32.exe" ]

\SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe Creates process:

0xffffffff]

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\UI0Detect.exe [C:\Windows\system32\UI0Detect.exe] Creates process: 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] C:\Windows\system32\svchost.exe [C:\Windows\system32\svchost.exe -k

Creates process: imgsvc]

Creates process: C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe]

Loads service: ALG [C:\Windows\System32\alg.exe]

Loads service: AppMgmt [C:\Windows\system32\svchost.exe -k netsvcs] BITS [C:\Windows\System32\svchost.exe -k netsvcs] Loads service:  $Browser \ [C:\Windows\System32\svchost.exe -k \ netsvcs]$ Loads service:

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]

EAPHost [C:\Windows\System32\svchost.exe -k netsvcs] Loads service: UIODetect [C:\Windows\system32\UIODetect.exe] Loads service:

Loads service: SharedAccess [C:\Windows\System32\svchost.exe -k netsvcs] Loads service: PNRPSvc [C:\Windows\System32\svchost.exe -k LocalServicePeerNet]

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:

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]

Schedule [C:\Windows\system32\svchost.exe -k netsvcs] Loads service:

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]

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:

Loads service: WUAUServ [C:\Windows\system32\svchost.exe -k netsvcs]

WLANSvc [C:\Windows\system32\svchost.exe -k Loads service:

LocalSystemNetworkRestricted]

PID:2372 C:\Windows\SysWOW64\calc.exe Reads from process:

C:\Windows\System32\alg.exe Terminates process: Terminates process: C:\Windows\System32\UI0Detect.exe C:\Windows\System32\VSSVC.exe Terminates process: C:\Windows\System32\svchost.exe Terminates process: C:\Windows\Temp\ToggleService32.exe Terminates process: Terminates process: C:\Windows\System32\conhost.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 C:\Windows\explorer.exe Creates remote thread: Creates remote thread: C:\Windows\System32\sppsvc.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex \BaseNamedObjects\MSDTC\_STATS\_EVENT Creates mutex:

Creates mutex: \BaseNamedObjects\DBWinMutex

Creates mutex: \BaseNamedObjects\{3f7f6ae1-db7c-4d2c-97cd-fc2604ee1135}\_S-1-5-19

\BaseNamedObjects\WIATRACE\_MUTEX Creates mutex:

Creates mutex: \BaseNamedObjects\{11517B7C-E79D-4e20-961B-75A811715ADD}

**\BaseNamedObjects\RouterPreInitEvent** Creates event:

 $\verb|\BaseNamedObjects\AudioSrv\_CanAcceptMMCClient|$ Creates event: Creates event:  $\verb|\BaseNamedObjects| WerSvcSystemPermissionsEvent|$ 

Creates event: **\BaseNamedObjects\WiaServiceStarted** 

Creates event: \BaseNamedObjects\99b25af4-39cf-4c83-ad07-3c133e6d3135 Creates event: \Sessions\1\BaseNamedObjects\PRS\_EXTERNAL\_CHECK\_CHANGED\_NOTIFY Creates event: \Sessions\1\BaseNamedObjects\{43a2b8d7-6fed-4c18-bd36-b4630d61afb5}

### File System Events

Creates: C:\Windows\SysWOW64\output.txt

Creates: C:\Windows\System32\MsDtc\Trace\dtctrace.log

C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat Creates: Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat Creates:

 ${\tt C:\Windows\Service\Profiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg}$ 

C:\ProgramData\Microsoft Creates: C:\ProgramData\Microsoft\Crypto Creates: C:\ProgramData\Microsoft\Crypto\RSA Creates:

Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys

Creates:

473a-b3d7-31d4d2573dc2

 $\verb|C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new| \\$ 

 ${\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst}$ 

C:\Windows\Debug\WIA Creates:

C:\Windows\ServiceProfiles\LocalService Creates:

Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Local

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows Creates:

Creates: C:\Windows\SoftwareDistribution Creates:

C:\Windows\System32\spp\store\data.dat.tmp  $C: \verb|\USers| Admin\\| AppData\\| Local\\| Microsoft\\| Windows\\| WER\\| ERC$ Creates:

Creates:  $\verb|C:\USers\Admin\AppData\Local\Microsoft\Windows\WER\ERC\statecache.lock| \\$ 

Creates: C:\Windows\System32\spp\store\cache\cache.dat C:\Windows\Prefetch\TOGGLESERVICE32.EXE-2248A864.pf Opens:

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysWOW64

C:\Windows\System32\conhost.exe Opens: C:\Windows\System32\combase.dll Opens: Opens:

C:\Windows\System32\en-US\conhost.exe.mui

C:\Windows\System32\ole32.dll Opens: Opens:  ${\tt C:\Windows\System32\uxtheme.dll}$ 

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\Windows\System32\dwmapi.dll Opens: C:\Windows\System32\en-US\user32.dll.mui

C:\Windows\system32\uxtheme.dll.Config Opens:

C:\Windows\WinSxS\amd64\_microsoft.windows.common-

controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_418c2a697189c07f

C:\Windows\WinSxS\amd64\_microsoft.windows.common-Opens: controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_418c2a697189c07f\comctl32.dll

C:\Windows\WindowsShell.Manifest Opens: Opens: C:\Windows\Svstem32\sechost.dll Opens: C:\Windows\System32\rpcss.dll Opens: C:\Windows\System32\cryptbase.dll C:\Windows\System32\bcryptprimitives.dll Opens: Opens:

C:\Windows\System32\SHCore.dll Opens: C:\Windows\SysWOW64\apphelp.dll C:\Windows\Temp\ToggleService32.exe Opens: C:\Windows\SysWOW64\ntdll.dll Opens: Opens: C:\Windows\SysWOW64\kernel32.dll Opens: C:\Windows\SysWOW64\KernelBase.dll C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\SysWOW64\sechost.dll Opens:

```
Opens:
                                       C:\Windows\SysWOW64\bcryptprimitives.dll
  Opens:
                                       C:\Windows\SysWOW64\cryptbase.dll
                                       C:\Windows\SysWOW64\sspicli.dll
  Opens:
  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
                                       C:\Windows\System32\mswsock.dll
  Opens:
  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
                                       C:\Windows\System32\msdtctm.dll
  Opens:
  Opens:
                                       C:\Windows\System32\msdtcprx.dll
  Opens:
                                       C:\Windows\System32\msdtclog.dll
  Opens:
                                       C:\Windows\System32\mtxclu.dll
  Opens:
                                       C:\Windows\System32\winmm.dll
                                       C:\Windows\System32\clusapi.dll
  Opens:
  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
                                       C:\Windows\System32\cryptdll.dll
  Opens:
  Opens:
                                       C:\Windows\System32\en-US\msdtc.exe.mui
  Opens:
                                       C:\Windows\System32\comres.dll
                                       C:\Windows\System32\msdtcVSp1res.dll
  Opens:
                                       C:\Windows\System32\mtxoci.dll
  Opens:
                                       C:\Windows\System32\MsDtc\Trace
  Opens:
                                       C:\Windows\System32\sspicli.dll
  Opens:
  Opens:
                                       C:\Windows\DtcInstall.log
  Opens:
                                       C:\Windows\System32\ntmarta.dll
  Opens:
                                       C:\Windows\System32\MsDtc
                                       C:\Windows\System32\MsDtc\MSDTC.LOG
  Opens:
  Opens:
                                       C:\Windows\System32\en-US\msdtcVSp1res.dll.mui
  Opens:
                                       C:\Windows\System32\FirewallAPI.dll
  Opens:
                                       C:\Windows\System32\winevt\Logs\Microsoft-Windows-
AppXDeploymentServer%4Operational.evtx
  Opens:
                                       C:\Windows\Svstem32\winevt\Logs\Microsoft-Windows-
NetworkProfile%4Operational.evtx
                                       C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
  Opens:
StoreMgr%4Operational.evtx
  Opens:
                                       C:\Windows\System32\winevt\Logs\Microsoft-Windows-
DeviceSetupManager%4Operational.evtx
                                       C:\Windows\System32\winevt\Logs\Microsoft-Windows-
  Opens:
UserPnp%4DeviceInstall.evtx
  Opens:
                                       C:\Windows\System32\UI0Detect.exe
  Opens:
                                       C:\Windows\Prefetch\UIODETECT.EXE-A794C8BB.pf
                                       C:\Windows\System32\wtsapi32.dll
  Opens:
  Opens:
                                       C:\Windows\System32\version.dll
  Opens:
                                       C:\Windows\System32\winsta.dll
  Opens:
                                       C:\Windows\System32\en-US\ui0detect.exe.mui
  Opens:
                                       C:\Windows\System32\adtschema.dll
  Opens:
                                       C:\Windows\System32\services.exe
  Opens:
                                       C:\Windows\ServiceProfiles
  Opens:
                                       C:\Windows\System32\svchost.exe
  Opens:
                                       C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
  Opens:
  Opens:
                                       C:\$Extend
                                       C:\ProgramData
  Opens:
                                       C:\ProgramData\Microsoft
  Opens:
                                       C:\ProgramData\Microsoft\Crypto
  Opens:
  Opens:
                                       C:\ProgramData\Microsoft\Crypto\RSA
  Opens:
                                       C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
  Opens:
                                       C:\Windows\Globalization
                                       C:\Windows\Globalization\Sorting
  Opens:
                                       C:\Windows\ServiceProfiles\LocalService
  Opens:
  Opens:
                                       C:\Windows\ServiceProfiles\LocalService\AppData
  Opens:
                                       C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
  Opens:
                                       C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My
  Opens:
C: \verb|\windows\Service| AppData \Roaming \verb|\wicrosoft| SystemCertificates \verb|\wy\Certificates| AppData \Roaming \verb|\wicrosoft| SystemCertificates \verb|\wy\Certificates| SystemCertificates| S
                                       C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
  Opens:
                                       C:\Windows\Svstem32\en-US
  Opens:
  Opens:
                                       C:\Windows\System32\ntdll.dll
                                       C:\Windows\System32\kernel32.dll
  Opens:
  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
```

C:\Windows\SysWOW64\msvcrt.dll

Opens:

```
Opens:
                         C:\Windows\System32\gpapi.dll
 Opens:
                         C:\Windows\System32\powrprof.dll
 Opens:
                         C:\Windows\System32\profapi.dll
                         C:\Windows\System32\crypt32.dll
 Opens:
 Opens:
                         C:\Windows\System32\msasn1.dll
 Opens:
C:\PROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\358129098041A0483A25B784E8E10913 DE228479-9E18-
473A-B3D7-31D4D2573DC2
                         C:\Windows\System32\en-US\crypt32.dll.mui
 Opens:
 Opens:
                         C:\Windows\System32\dpapi.dll
                         C:\Windows\System32\ncrypt.dll
 Opens:
 Opens:
                         C:\Windows\System32\ntasn1.dll
 Opens:
                         C:\Windows\System32\QAGENTRT.DLL
 Opens:
                         C:\Windows\System32\en-US\QAgentRT.dll.mui
                         C:\Windows\System32\en-US\dnsapi.dll.mui
 Opens:
                         C:\Windows\System32\fveui.dll
 Opens:
 Opens:
                         C:\Windows\System32\en-US\fveui.dll.mui
 Opens:
                         C:\Windows\System32\wuaueng.dll
                         C:\Windows\System32\en-US\wuaueng.dll.mui
 Opens:
 Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
 Opens:
                         C:\Windows\System32\advapi32.dll
 Opens:
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst}
 Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
                         C:\Windows\System32\ws2_32.dll
 Opens:
                         C:\Windows\System32\nsi.dll
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
 Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\Windows\System32\dhcpcsvc6.dll
 Opens:
                         C:\Windows\System32\dhcpcsvc.dll
                         C:\Windows\System32\sqmapi.dll
 Opens:
                         C:\Windows\System32\gdi32.dll
 Opens:
 Opens:
                         C:\Windows\System32\en-US\svchost.exe.mui
                         C:\Windows\System32\oleaut32.dll
 Opens:
 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
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\4601d02f1df7da88667245cbda62ad09_de228479-9e18-
473a-b3d7-31d4d2573dc2
 Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\41463ec372023a3ac6aa99233b535a52 de228479-9e18-
473a-b3d7-31d4d2573dc2
 Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\0eb913b970672c404f64141ce3de942e.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\drivers\etc\lmhosts
 Opens:
                         C:\Windows\System32\VSSVC.exe
                         C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
 Opens:
 Opens:
                         C:\Windows\System32\vssapi.dll
 Opens:
                         C:\Windows\System32\vsstrace.dll
 Opens:
                         C:\Windows\System32\virtdisk.dll
                         C:\Windows\System32\dsrole.dll
 Opens:
 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
                         C:\Windows\System32\samlib.dll
 Opens:
                         C:\Windows\System32\es.dll
 Opens:
 Opens:
                         C:\Windows\System32\propsys.dll
 Opens:
                         C:\Windows\System32\catsrvut.dll
 Opens:
                         C:\Windows\System32\mfcsubs.dll
                         C:\Windows\System32\sxs.dll
 Opens:
 Opens:
                         C:\Windows\System32\eventcls.dll
 Opens:
                         C:\Windows\System32\stdole2.tlb
                         C:\Windows\System32\msxml3.dll
 Opens:
                         C:\Windows\System32\shlwapi.dll
 Opens:
 Opens:
                         C:\Windows\System32\en-US\KernelBase.dll.mui
 Opens:
                         C:\Windows\System32\msxml3r.dll
 Opens:
                         C:\Windows\System32\setupapi.dll
                         C:\Windows\System32\cfgmgr32.dll
 Opens:
```

```
Opens:
                                                                                                                        C:\Windows\System32\devobj.dll
         Opens:
                                                                                                                        C:\Windows\System32\en-US\setupapi.dll.mui
         Opens:
                                                                                                                        C:\Windows\System32\wintrust.dll
                                                                                                                        C:\Windows\System32\audiosrv.dll
         Opens:
         Opens:
                                                                                                                        C:\Windows\System32\hid.dll
                                                                                                                        C:\Windows\System32\avrt.dll
        Opens:
                                                                                                                        C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
         Opens:
        Opens:
                                                                                                                        C:\Windows\System32\wersvc.dll
                                                                                                                        C:\Windows\System32\dps.dll
         Opens:
        Opens:
                                                                                                                        C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
DPS%4Operational.evtx
         Opens:
                                                                                                                        C:\Windows\System32\diagperf.dll
                                                                                                                        C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-
        Opens:
 Performance%40perational.evtx
                                                                                                                        C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
         Opens:
                                                                                                                        C:\Windows\debug
         Opens:
         Opens:
                                                                                                                        C:\Windows\debug\WIA
        Opens:
                                                                                                                        C:\Windows\System32\wiaservc.dll
                                                                                                                        C:\Windows\System32\wiatrace.dll
        Opens:
                                                                                                                        C:\Windows\System32\msv1_0.dll
        Opens:
                                                                                                                        C:\Windows\System32\sti.dll
        Opens:
         Opens:
                                                                                                                        C:\Windows\debug\WIA\wiatrace.log
        Opens:
                                                                                                                        C: \verb|Windows\System32\LogFiles\Scm\e5918cb5-cb06-4d74-80c7-8dd0399361c4|
         Opens:
                                                                                                                        C:\Windows\System32\LogFiles\Scm\26c02f2c-5d20-44dd-b03f-e87f8ff3ea9b
         Opens:
                                                                                                                        C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
                                                                                                                        C:\Windows\System32\Drivers\nwifi.sys
         Opens:
         Opens:
                                                                                                                        C:\Windows\apppatch\drvmain.sdb
         Opens:
                                                                                                                        C:\Windows\System32\Drivers\ndisuio.sys
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
         Opens:
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
         Opens:
                                                                                                                        C: \verb|\windows\System32\catroot| F750E6C3-38EE-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-
00C04FC295EE\} \\ Microsoft-Hyper-V-Common-Drivers-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Hyper-V-Management-Clients-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim e
US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                        C: \verb|Windows\System32\catroot| F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5
{\tt 00C04FC295EE} \verb+\Microsoft-Hyper-V-Management-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-PowerShell-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Hyper-V-Management-PowerShell-Package \\ ^{31b}f3856ad364e35 \\ ^{2}amd64 \\ ^{2}en-Package \\ ^{3}berrore \\ ^{3}berro
US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Hyper-V-Package-minkernel-31bf3856ad364e35-amd64--6.2.9200.16384.cat \\ Control of the control of t
        Opens:
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package-31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Hyper-V-Server-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim 6.2.9200.16384. \\ categories \\ categories \\ \sim 6.2.9200.16384. \\ catego
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Media-Foundation-Package ~31bf3856ad364e35 ~amd64 ~en-US~6.2.9200.16384. \\ category ~2.9200.16384. \\ category ~2.9200. \\ category ~2.9200. \\ category ~2.9200. \\ category ~2.9200. \\ category ~2.9200.
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Media-Foundation-Package ~ 31bf3856ad364e35 \\ \\ -amd64 \\ -~6.2.9200.16384. \\ categorian \\ cate
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Virtualization-Client-Interop-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
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
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-
```

```
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3856ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-en-AvCore-Package-31bf3866ad364e35-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-a
 US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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
                                                                                                                                    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: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                    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
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-ApisetNamespace-Minio-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-10cm \\ \sim 10cm \\ \sim 
US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 \tt 00C04FC295EE\} \verb+\Microsoft-Windows-ApisetNamespace-Minio-Pair ApisetNamespace-Minio-Pair ApisetNam
 Package \sim 31bf 3856 ad 364 e 35 \sim amd 64 \sim -6.2.9200.16384. cat
         Opens:
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3856ad364e35~amd64~en-Minkernel-Package~31bf3866ad364e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~a
 US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 US~6.2.9200.16384.cat
         Opens:
                                                                                                                                    C: \verb|Windows\System32\catroot| F750E6C3-38EE-11D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5-12D1-85E5
 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-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-Microsoft-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Window
 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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-Windows-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~en-Microsoft-Windows-ApisetNamespace-Windows-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\
 US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-
 Package \sim 31bf 3856 ad 364 e 35 \sim amd 64 \sim \sim 6.2.9200.16384.cat
         Opens:
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-W0W64-AvCore-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-10c0 \\ \sim 10c0 \\ \sim 
 US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
  00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
 Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-WOW64-Com-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~en-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~am
 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
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 US~6.2.9200.16384.cat
                                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 {\tt 00C04FC295EE} \verb+\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-Power States} \\
```

```
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
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
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-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
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
US~6.2.9200.16384.cat
                                                   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 \\ \sim \\ 31bf3856ad364e35 \\ \sim \\ amd64 \\ \sim \\ 6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
Opens:
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \texttt{Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd
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
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
US~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Branding-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Branding-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Branding-Professional WMC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Microsoft-Windows-Branding-Professional WMC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Microsoft-Windows-Branding-Professional WMC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Microsoft-Windows-Branding-Professional WMC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Microsoft-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Branding-Windows-Windows-Branding-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Win
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
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Business Scanning-Feature-Package-admin~31bf3856ad364e35~amd64~en-defendant for the control of the cont
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
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
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-drivers-21bf3856ad364e35\\ \\ -amd64\\ \\
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Client-Drivers-Package-multimedia-$31bf3856ad364e35-amd64-en-confidence of the confidence of the
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
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE\} \\ Microsoft-Windows-Client-Drivers-Package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364e35-amd64-en-drivers-package-printscan-31bf3856ad364-en-drivers-package-printscan-31bf3856ad364-amd64-en-drivers-package-printscan-31bf3856ad364-amd64-en-drivers-package-printscan-31bf3856ad364-amd64-en-drivers-package-printscan-31bf3856ad364-amd64-en-drivers-package-printscan-31bf3856ad364-amd64-en-drivers-package-printscan-31bf3856ad364-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd
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
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Client-Drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3866ad364e35-amd64-en-drivers-Package-termsrv-31bf3866ad364e35-amd64-en-drivers-Package-termsrv-31bf3866ad364e35-amd64-en-drivers-Package-termsrv-31bf3866ad364e35-amd646-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64
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
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE \} \\ Microsoft-Windows-Client-Drivers-Package \\ ^{31bf3856ad364e35} \\ ^{amd64} \\ ^{en-Drivers-Package} \\ ^{31bf3856ad364e35} \\ ^{31bf386ad364e35} \\ ^{31bf386ad364} \\ ^{
US~6.2.9200.16384.cat
       Opens:
                                                                                                C: \verb|\windows\System32\catroot| F750E6C3-38EE-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-85E5-| F750E6C3-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-11D1-88E-
00C04FC295EE\} \\ Microsoft-Windows-Client-Drivers-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                                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
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
\verb|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
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
 inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
       Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
```

```
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64~en-minio~31bf3856ad364e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e3
US~6.2.9200.16384.cat
                                                                            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
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package-multimedia ~31bf3856ad364e35 \\ \\ -amd64-en-multimedia ~31bf3856ad364e35 \\ \\ -amd64-en-multimedia \\ \\ -amd64-e
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
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            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
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                           C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
     Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
 termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ \label{limit} Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-limits-lim
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Client-Language Pack-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-10c04FC295EE \\ \sim 10c04FC295EE \\ \sim 10c
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-COM-MSMQ-package-31bf3856ad364e35-amd64--6.2.9200.16384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.16384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364e35-amd64--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364--6.2.9200.06384.cat} \\ \mbox{Com-mSMQ-package-31bf3856ad364--6.2.0000.cat} \\ \mbox{Com-mSMQ-package-31bf3866ad
                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-
```

```
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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
                                                                                                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE\} \\ \ Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers-Package-admin~amd64~en-drivers
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
                                                                                                                                                                              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-ended from the common of the common of
 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: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-12B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E5-14B1-85E
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
 ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                                              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
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE\} \\ Microsoft-Windows-Common-Drivers-Package-minkernel \\ \sim 31bf3856ad364e35\\ \sim amd64\\ \sim en-Drivers-Package-minkernel \\ \sim 31bf3856ad364\\ \sim amd64\\ \sim amd6
US~6.2.9200.16384.cat
            Opens:
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \ Microsoft-Windows-Common-Drivers-Package-net \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endowner \\ \sim amd 64 \\ \sim am
 US~6.2.9200.16384.cat
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
 net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE\} \\ Microsoft-Windows-Common-Drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3856ad364e35-amd64-en-drivers-Package-termsrv-31bf3866ad36-amd64-en-drivers-Package-termsrv-31bf3866-amd64-en-drivers-Package-termsrv-31bf3866-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd6
 US~6.2.9200.16384.cat
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
 termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-Common-Drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364e35-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3856ad364-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drivers-Package-vm-31bf3864-amd64-en-drive
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
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \ Microsoft-Windows-Common-Drivers-Package-windows-31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bright \\ \sim amd 64 \\ \sim amd 64 \\ \sim en-bright \\ \sim amd 64 \\
 US~6.2.9200.16384.cat
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 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
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE\} \\ Microsoft-Windows-Common-Modem-Drivers-Package-net \\ ~31bf3856ad364e35\\ ~amd64\\ ~en-drivers-Package-net \\ ~31bf3856ad364e35\\ ~amd64\\ ~amd64\\
 US~6.2.9200.16384.cat
                                                                                                                                                                              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 \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Modem-Drivers-Package \\ \sim amd 64 \\ 
 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
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 00C04FC295EE\} \\ Microsoft-Windows-CommonFoundation-LanguagePack-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-10cm \\ \sim 10cm \\ \sim
 US~6.2.9200.16384.cat
            Opens:
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-CoreSystem-Base-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim ende
 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
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 US~6.2.9200.16384.cat
                                                                                                                                                                              C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
            Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
            Opens:
 US~6.2.9200.16384.cat
             Opens:
                                                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE\} \\ Microsoft-Windows-CoreSystem-DS-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^c6.2.9200.16384.cat
                                                                                         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
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-CoreSystem-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Minio-Package \\ \sim amd64 \\ \sim am
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-
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
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-CoreSystem-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-Package \\ \sim amd 64 \\ \sim a
US~6.2.9200.16384.cat
       Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\}\\ Microsoft-Windows-CoreSystem-Package ~31bf3856ad364e35 ~amd 64 ~~ 6.2.9200.16384. cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
      Opens:
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \verb|\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-defection | 100C04FC295EE \\ |\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-defection | 100C04FC295EE \\ |\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e36~amd64~en-defection | 100C04FC295EE \\ |\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-defection | 100C04FC295EE \\ |\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-defection | 100C04FC295EE \\ |\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856~amd64~en-defection | 100C04FC295
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
                                                                                         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
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-CoreSystem-WOW64-DS-}
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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-
{\tt OOCO4FC295EE} \verb+\Microsoft-Windows-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-WOW64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreSystem-Wow64-Minio-CoreS
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
      Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ Microsoft-Windows-CoreSystem-WOW64-Net-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364e35-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3856ad364-amd64-en-Package~31bf3866ad364-amd64-en-Package~31bf3866ad364-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-a
US~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-CoreSystem-WOW64-Net-Point} \\
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                      C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
 00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      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
                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                                                      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
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim 6.2.9200.16384.cat
      Opens:
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Editions-Professional-Package} \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-brownessional \\ \sim amd64 \\ \sim en-brownessional \\ \sim amd64 \\ 
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Editions-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-Comparison} \\
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-GroupPolicy-ClientExtensions-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-100c04FC295EE \\ \sim 100c04FC295EE \\ \sim 100c04FC2
US~6.2.9200.16384.cat
                                                                                      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-defined by the contraction of the contraction 
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-GroupPolicy-ClientTools-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Packag
\verb|com-31bf3856ad364e35-amd64--6.2.9200.16384.cat|\\
                                                                                      C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
```

```
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-GroupPolicy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-ClientTools-Package-Policy-Policy-ClientTools-Package-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-Policy-P
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              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
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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-defined by the control of 
US~6.2.9200.16384.cat
                                                              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
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-GroupPolicy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-ClientTools-Package-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Four-Policy-Fo
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
                                                              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
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Help-ClientUA-Professional \\ \ MC-Package-31bf3856ad364e35-amd64-en-Microsoft-Windows-Help-ClientUA-Professional \\ \ MC-Package-31bf3856ad364e35-amd64-en-Microsoft-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Wind
US~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
```

```
00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-ICM-Package~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
00C04FC295EE\} \\ Microsoft-Windows-Identity-Foundation-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^en-Backage \\ ^31bf3856ad364e35 \\ ^amd64 \\ 
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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Add0n-2-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Add0n-2-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE \} \\ Microsoft-Windows-IIS-WebServer-AddOn-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~en-Backage \\ ~31bf3856ad364e35 \\ ~amd64 \\
US~6.2.9200.16384.cat
        Opens:
                                                                                                                                   C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   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\} \\ \texttt{Microsoft-Windows-IIS-WebServer-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat}
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBa
Base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE\}\\ Microsoft-Windows-ImageBasedSetup-IE-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364e35~amd64~en-Package-windows-31bf3856ad364~amd64~en-Package-windows-31bf3856ad364~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3856~amd64~en-Package-windows-31bf3866~amd64~en-Package-windows-31bf3866~amd646~amd646~amd64~amd646~amd646~amd646~amd646~amd64~amd646~amd646~amd646~amd646~amd646~
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-IE-Package-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-III-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-II-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBasedSetup-ImageBa
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
00C04FC295EE\} \\ Microsoft-Windows-InternetExplorer-Optional-Package \\ ~31bf3856ad364e35 \\ ~amd 64 \\ ~en-Details \\ ~amd 64 \\ ~en-Details \\ ~amd 64 \\ ~amd 6
US~10.0.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
                                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-InternetExplorer-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Pac
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~en-defined by the control of the contro
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Windows-Killbits-Package-31bf3856ad364e35-amd64--10.0.9200.16384.cat \\ Cathering and Control of the Control of th
                                                                                                                                   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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-Media-Format-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-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
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
.00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                 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
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-MediaPlayer-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim 6.2.9200.16384.cat
    Opens:
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64~en-Basic-Package~31bf3856ad364e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd64e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~amd66e35~
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Onens:
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-defined by the control of 
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-MobilePC-Client-Premium-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-Premium-MobilePC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-PC-Client-
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
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ Microsoft-Windows-MobilePC-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Client-SideShow-Package \\ \sim amd64 \\ \sim am
US~6.2.9200.16384.cat
                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-
```

```
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                   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
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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 \sim 31bf3856ad364e35 \sim amd64 \sim 6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                   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
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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\} \\ \mbox{Microsoft-Windows-Multilingual-Package-shell} \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-100c04FC295EE \\ \sim 100c04FC295EE \\ \sim 100c04FC295EE
US~6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                  C: \verb|\windows\\System32\\catroot\\\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
    Opens:
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
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-
AutoNgenEnable.3.5~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295FF}\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
                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                   C: \verb|Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5
    Opens:
00C04FC295EE\} \\ \texttt{Microsoft-Windows-NetFx-Shared-Package-31bf3856ad364e35-amd64\sim-6.2.9200.16384.cat} \\ \texttt{Cather Shared-Package-31bf3856ad364e35-amd64\sim-6.2.9200.16384.cat} \\ \texttt{Cather Shared-Package-31bf3856ad364e35-amd6400.06300.cat} \\ \texttt{Cather Shared-Package-31bf3866ad364e35-amd6400.06300.cat} \\ \texttt{Cather Shared-Package-31bf3866ad364e35-amd6400.06300.cat} \\ \texttt{Cather Shared-Package-31bf3866ad364e35-amd6400.06300.cat} \\ \texttt{Cather Shared-Package-31bf3866ad3640.cat} \\ \texttt{Cather Shared-Package-31bf38660.cat} \\ \texttt{Cather Shared-Package-31bf3860.cat} \\ \texttt{Cath
    Opens:
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ Microsoft-Windows-NetFx-Shared-Typelibs~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpNamespace \sim\! 31bf3856ad364e35 \sim\! amd64 \sim\! \sim\! 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
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
 TcpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
 TcpPortSharing~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE \} \\ \label{lem:condition} Microsoft-Windows-NetFx-Shared-WPF-Package $$^31bf3856ad364e35$$ amd $64$$en-100C04FC295EE $$$ $$^31bf3856ad364e35$$ and $64$$$ en-100C04FC295EE $$$$ $$^31bf3856ad364e35$$ and $64$$$ en-100C04FC295EE $$$ $$^31bf3856ad364e35$$ and $64$$ en-100C04FC295EE $$$ and $64$$ en-100C04FC295EE 
US~6.2.9200.16384.cat
        Opens:
                                                                                                       C: \verb|Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5
 00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                       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
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE \} \\ \text{Microsoft-Windows-NetFx2-OC-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \text{Constant of the property of the 
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE\} \\ Microsoft-Windows-NetFx2-OC-Package \\ ~31bf3856ad364e35 \\ ~amd \\ 64 \\ ~6.2.9200.16384.cate \\ ~6.2.9200.cate \\ ~6.2.9200.cate \\ ~6.2.9200.cate 
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package-
 redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
       Opens:
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-NetFx3-0C-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
       Opens:
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 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 \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-NetFx4-US-OC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ 
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
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
US~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                      C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
       Opens:
 00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-OfflineFiles-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e35-amd64-en-files-UI-Package-31bf3856ad364e3-amd64-en-files-UI-Package-31bf3856ad364e3-amd64-en-files-UI-Package-31bf3866ad364e3-amd64-en-files-UI-Package-31bf3866ad364e3-amd64-en-files-UI-Package-31bf3866ad36-amd64-en-files-UI-Package-31bf3866ad36-amd64-en-files-UI-Package-31bf3866ad36-amd64-en-files-UI-Package-31bf3866ad36-amd64-en-files-UI-Package-31bf3866ad36-amd64-en-files-UI-Package-31bf3866ad36-en-files-UI-Package-31bf3866ad36-en-files-UI-Package-31bf3866ad36-en-files-UI-Package-31bf3866ad36-en-files-UI-Package-31bf3866ad36-en-files-UI-Package-31bf38666ad36-en-files-UI-Package-31bf386666ad36-en-files-UI-Package-31bf38666-en-files-UI-Package-31bf386666-en-files-
US~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE}\Microsoft-Windows-ParentalControls-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
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
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
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
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE}\Microsoft-Windows-Personalization-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\}\\ Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
.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 \\
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Portable-Devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-Package-windows-31bf3856ad364e35-amd64-en-devices-package-windows-31bf3856ad364e35-amd64-en-devices-package-windows-31bf3856ad364e35-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-package-windows-amd64-en-devices-pa
US~6.2.9200.16384.cat
                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
```

```
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
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
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    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
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-Printer-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-Printing-LocalPrinting-Home-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE \} \\ \label{lem:condition} \begin{tabular}{ll} \begi
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
                                                    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
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE\} \\ Microsoft-Windows-Professional WMCE dition-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
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
   Opens:
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ \mbox{Microsoft-Windows-RDC-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \mbox{Continuous-RDC-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \mbox{Continuous-RDC-Package-31bf3856ad364-en-US-6.2.9200.cat} \\ \mbox{Continuous-RDC-Package-31bf3856ad364-en-US-6.2.0000.cat} \\ \mbox{Continuous-RDC-Package-31bf3856ad364-en-US-6.2.0000.cat} \\ \mbox{Cont
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-RDC-Package \\ \sim 31bf3856ad364e35-amd64 \\ \sim 6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00c04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ \ Microsoft-Windows-Remote Assistance-Package-Client \sim 31bf3856 ad 364e 35 \sim amd 64 \sim en-1000 and 1000 ad 1000 and 1000 ad 
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
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
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-
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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
                                                                                          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
                                                                                         C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
      Opens:
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\}\\ Microsoft-Windows-Secure Startup-Package ~31bf3856ad364e35 ~amd 64 ~~ 6.2.9200.16384. cat a constant of the c
                                                                                         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
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-0CUR-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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
                                                                                         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
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C: \verb|\windows\\System32\\catroot\\\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
      Opens:
US~6.2.9200.16384.cat
      Opens:
                                                                                          C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
 00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                         C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
 00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
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
                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~en-decomposition for the contraction of the contraction
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
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~en-defined by the contraction of the c
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\}\\ \ Microsoft-Windows-SKU-Foundation-Package-base~31bf3856ad364e35~amd64~en-base and a substitution of the control of the cont
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
```

```
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ \label{lem:condition} Microsoft-Windows-SKU-Foundation-Package-ds-31bf3856ad364e35-amd64-en-data for the condition of the co
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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
                                                                                                                                   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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf3856ad364e35-amd64-en-foundation-package-inetsrv-31bf386ad364e35-amd64-en-foundation-package-inetsrv-31bf386ad364e35-amd64-en-foundation-package-inetsrv-31bf386ad364e35-amd64-en-foundation-package-inetsrv-31bf386ad364e35-amd64-en-foundation-package-inetsrv-31bf386ad364e35-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad364e36-amd64-en-foundation-package-inetsrv-31bf386ad366-amd64-en-foundati
 US~6.2.9200.16384.cat
         Opens:
                                                                                                                                   C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
 {\tt 00C04FC295EE} \verb+\Microsoft-Windows-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-Foundation-Package-SKU-F
  inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   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
                                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 . 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
 mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
         Opens:
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3856ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd64-en-minkernel-31bf3866ad364e35-amd646-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-net~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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-data for the control of the co
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
  00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
 sdktools~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-shell~31bf3856ad364e35~amd64~en-defined by the contraction of the co
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-sql-$31bf3856ad364e35-$amd64-en-lember 1.00cm.} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-sql-$31bf3856ad364-$amd64-en-lember 1.00cm.} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-sql-$31bf3866ad364-$amd64-en-lember 1.00cm.} \\ \mbox{Micros
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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE\} \\ \ Microsoft-Windows-SKU-Foundation-Package-termsrv-31bf3856ad364e35-amd64-en-defined by the state of the
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-windows-31bf3856ad364e35-amd64-en-defined by the control of the con
 US~6.2.9200.16384.cat
                                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3856ad364e35-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364e35-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364e35-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364e35-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364e36-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364e36-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364e36-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad364-amd64-en-2000} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-31bf3866ad36-amd64-en-2000} \\ \mbox{Micr
```

```
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\}\\ Microsoft-Windows-SKU-Foundation-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-SNMP-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \mbox{Continuous-SNMP-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \mbox{Continuous-SNMP-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.0000.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3866ad364e35-amd64-en-US-6.2.9200.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3866ad364e35-amd64-en-US-6.2.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3866ad364e35-amd64-en-US-6.2.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3866ad364e35-amd64-en-US-6.2.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3866ad364e35-amd64-en-US-6.2.0000.cat} \\ \mbox{Continuous-SNMP-Package-31bf3866ad364-amd64-en-US-6.0000.cat} \\ \mbox{Continuous-SNMP-Package
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-SNMP-Package-31bf3856ad364e35-amd64-$\sim$6.2.9200.16384.cat}
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-SpeechRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ Microsoft-Windows-SystemRestore-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^c6.2.9200.16384. cat \\ ^backage \\ ^abf3856ad364e35 \\ ^amd64 \\ ^c6.2.9200.16384. cat \\ ^backage \\ ^abf3856ad364e35 \\ ^amd64 \\ ^c6.2.9200.16384. cat \\ ^backage \\ ^abf3856ad364e35 \\ ^amd64 \\ ^c6.2.9200.16384. cat \\ ^amd64 \\ ^amd6
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ \texttt{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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ Microsoft-Windows-Terminal Services-WMIProvider-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-10cm \\ \sim 10cm \\ \sim
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
                                                        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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ Microsoft-Windows-TFTP-Client-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
   Opens:
00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \verb|Microsoft-Windows-WindowsFoundation-LanguagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-Package-31bf3856ad364e35-amd64-en-languagePack-31bf3856ad364-amd64-en-languagePack-31bf3856ad364-amd64-en-languagePack-31bf3856ad364-amd64-amd64-en-languagePack-31bf3866ad364-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-am
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                 C: \verb|\windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E
     Opens:
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 \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage-avcore \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage-avcore \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage-avcore \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage-avcore \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage-avcore \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage-avcore \\ \sim amd64 \\ \sim amd
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\}\\ Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-WinSATMediaFiles-
Package \sim 31bf 3856 ad 364 e 35 \sim amd 64 \sim -6.2.9200.16384. cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 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
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-WMPNetworkSharingService-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim endownerse \\ \sim amd64 \\ \sim amd64 \\ \sim endownerse \\ \sim amd64 \\ \sim amd64 \\ \sim endownerse \\ \sim endowners
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Xps-Foundation-Client-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^en-Backage \\ ^31bf3856ad364e35 \\ ^amd64 
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\nt5.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\ntexe.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Windows-Defender-AM-Default-Definitions-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\windows-legacy-whql.cat
                                                                                 C:\Windows\System32\kerberos.dll
     Opens:
      Opens:
                                                                                  C:\Windows\System32\wlanapi.dll
                                                                                  C:\Windows\System32\wlanhlp.dll
     Opens:
                                                                                  C:\Windows\System32\SubscriptionMgr.dll
      Opens:
                                                                                  C:\Windows\System32\wevtapi.dll
     Opens:
                                                                                  C:\Windows\System32\winevt\Logs\Microsoft-Windows-
      Opens:
Wcmsvc%40perational.evtx
      Opens:
                                                                                  C:\Windows\System32\dpapisrv.dll
      Opens:
                                                                                  C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
DPAPI%4Operational.evtx
      Opens:
                                                                                  C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
```

```
DPAPI%4BackUpKeySvc.evtx
                         C:\Windows\System32\wlansvc.dll
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-
  Opens:
AutoConfig%4Operational.evtx
 Opens:
                         C:\Windows\System32\catroot2
                         C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
  Opens:
                         C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
 Opens:
00C04FC295EE}\catdb
                         C:\Windows\system32\CatRoot2\{127D0A1D-4EF2-11D1-8608-
 Opens:
00C04FC295EE}\catdb\
  Opens:
                         C:\Windows\system32\CatRoot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
  Opens:
                         C:\Windows\system32\CatRoot2
  Opens:
                         C:\Windows\system32
  Opens:
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-
  Opens:
00C04FC295EE}\catdb
 Opens:
                         C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\catdb\
                         C:\Windows\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
 Opens:
  Opens:
                         C:\Windows\System32\catroot2\edb.chk
 Opens:
                         C:\Windows\System32\catroot2\edb.log
                         C:\Windows\system32\CatRoot2\res1.log
  Opens:
 Opens:
                         C:\Windows\system32\CatRoot2\res2.log
  Opens:
                         C:\Windows\System32\catroot
  Opens:
                         C:\
                         C:\Windows\Temp
  Opens:
  Opens:
                         C:\Windows\Temp\ToggleService32.exe\
                         C:\Windows\System32\sppsvc.exe
  Opens:
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  Opens:
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 Opens:
00C04FC295EE}\Microsoft-Windows-Common-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
  Opens:
  Opens:
                         C:\Windows\Branding
                         {\tt C:\Windows\Branding\Basebrd}
  Opens:
 Opens:
                         C:\Windows\System32\en-US\sppsvc.exe.mui
  Opens:
                         C:\Windows\System32\sppobjs.dll
  Opens:
                         C:\Windows\Branding\Basebrd\basebrd.dll
                         C:\Windows\System32\wwapi.dll
  Opens:
                         C:\Windows\System32\wscsvc.dll
  Opens:
  Opens:
                         C:\Windows\System32\dbghelp.dll
  Opens:
                         C:\Windows\System32\wbem\wbemprox.dll
 Opens:
                         C:\Windows\System32\wbemcomn.dll
  Opens:
                         C:\Windows\System32\wbem\wbemsvc.dll
                         C:\Windows\System32\wbem\fastprox.dll
 Opens:
                         C:\Windows\System32\winhttp.dll
 Opens:
  Opens:
                         C:\Windows\System32\wuapi.dll
  Opens:
                         C:\Windows\System32\cabinet.dll
  Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\WindowsUpdate.log
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\WindowsUpdate.log\
  Opens:
                         C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows
  Opens:
                         C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft
  Opens:
                         C:\Windows\ServiceProfiles\LocalService\AppData\Local
                         C:\Windows\System32\wups.dll
 Opens:
                         C:\Windows\System32\ci.dll
  Opens:
 Opens:
                         C:\Windows\System32\userenv.dll
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
  Opens:
CodeIntegrity%4Operational.evtx
  Opens:
                         C:\Windows\System32\wkscli.dll
  Opens:
                         C:\Windows\System32\spp\store\data.dat
  Opens:
                         C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
```

```
Opens:
                          C:\Windows\System32\sppwinob.dll
 Opens:
                          C:\Windows\System32\netapi32.dll
 Opens:
                          C:\Windows\System32\srvcli.dll
 Opens:
                          C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
manifest-signed.xrm-ms
                          C:\Windows\Svstem32\spp\store\cache\cache.dat
 Opens:
 Opens:
                          C:\Windows\System32\spp\store\tokens.dat
                          C:\Windows\System32\spp\store\data.dat.tmp
 Opens:
                          C:\Windows\System32\spp\store
 Opens:
                          {\tt C:\Windows\System32\spp\store\data.dat.bak}
 Opens:
 Opens:
                          C:\Windows\System32\msxml6.dll
 Opens:
                          C:\Windows\System32\msxml6r.dll
 Opens:
                          C:\Windows\System32\taskschd.dll
 Opens:
                          C:\Windows\System32\wscinterop.dll
                          C:\Windows\System32\wscapi.dll
 Opens:
                          C:\Windows\System32\wscui.cpl
 Opens:
 Opens:
                          C:\Windows\System32\wscinterop.dll.123.Manifest
 Opens:
                          C:\Windows\System32\en-US\wscui.cpl.mui
                          C:\Windows\System32\werconcpl.dll
 Opens:
                          C:\Windows\System32\wer.dll
 Opens:
                          C:\Windows\System32\framedynos.dll
 Opens:
 Opens:
                          C:\Windows\System32\wercplsupport.dll
 Opens:
                          {\tt C:\Wers\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive}
 Opens:
                          C:\ProgramData\Microsoft\Windows\WER\ReportArchive
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
                          C:\Windows\System32\hcproviders.dll
 Opens:
                          C:\Windows\System32\en-US\hcproviders.dll.mui
 Opens:
 Opens:
                          C:\Windows\System32\en-US\ActionCenter.dll.mui
 Opens:
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
WindowsBackup%4ActionCenter.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Opens:
NetworkAccessProtection%4WHC.evtx
 Opens:
                          C:\Windows\Svstem32\winevt\Logs\Microsoft-Windows-Windows
Defender%4WHC.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
 Opens:
Scheduled%40perational.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Opens:
TaskScheduler%4Maintenance.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Control
 Opens:
Panel%40perational.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-
 Opens:
Notifications%4ActionCenter.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-
 Opens:
Core%4WHC.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
 Opens:
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-
 Opens:
ConnectedAccountState%4ActionCenter.evtx
 Opens:
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
UserPnp%4ActionCenter.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-
 Opens:
ManagementAgent%4WHC.evtx
 Opens:
                          C:\Windows\System32\Actioncenter.dll.3.Manifest
 Opens:
                          C:\Windows\System32\umpnpmgr.dll
                          C:\Windows\SysWOW64\output.txt
 Writes to
 Writes to:
                          C:\Windows\System32\MsDtc\Trace\dtctrace.log
                          C:\Windows\System32\MsDtc\MSDTC.LOG
 Writes to:
 Writes to:
                          C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
                          {\tt C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat}
 Writes to:
 Writes to:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
 Writes to:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\41463ec372023a3ac6aa99233b535a52_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
 Writes to:
                          C:\Windows\System32\catroot2\edb.log
                          C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
 Writes to:
00C04FC295EE}\catdb
                          C:\Windows\Svstem32\catroot2\{F750E6C3-38EE-11D1-85E5-
 Writes to:
00C04FC295EE}\catdb
 Writes to:
                          C:\Windows\System32\spp\store\data.dat.tmp
 Writes to:
                          C:\Windows\System32\spp\store\cache\cache.dat
 Reads from:
                          C:\Windows\SysWOW64\output.txt
  Reads from:
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
AppXDeploymentServer%4Operational.evtx
 Reads from:
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
NetworkProfile%4Operational.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
 Reads from:
StoreMgr%4Operational.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
DeviceSetupManager%4Operational.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Reads from:
UserPnp%4DeviceInstall.evtx
 Reads from:
                          C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
 Reads from:
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst}
{\tt C:\Windows\Service\Profiles\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\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
DPS%40perational.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-
Performance%40perational.evtx
 Reads from:
                         C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
                         C:\Windows\System32\LogFiles\Scm\e5918cb5-cb06-4d74-80c7-8dd0399361c4
 Reads from:
                         C: \verb|\windows\System32\LogFiles\Scm\26c02f2c-5d20-44dd-b03f-e87f8ff3ea9b| \\
 Reads from:
                         C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
 Reads from:
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
Wcmsvc%40perational.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
DPAPI%4Operational.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
 Reads from:
DPAPI%4BackUpKeySvc.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-
AutoConfig%4Operational.evtx
                         C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
 Reads from:
00C04FC295EE}\catdb
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-
 Reads from:
00C04FC295EE}\catdb
 Reads from:
                         C:\Windows\System32\catroot2\edb.log
 Reads from:
                         C:\Windows\System32\catroot2\edb.chk
 Reads from:
                         C:\Windows\Temp\ToggleService32.exe
 Reads from:
                         C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
CodeIntegrity%4Operational.evtx
 Reads from:
                         C:\Windows\System32\spp\store\data.dat
 Reads from:
                         C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
 Reads from:
                         C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
manifest-signed.xrm-ms
                         C:\Windows\System32\spp\store\cache\cache.dat
 Reads from:
                         C:\Windows\System32\spp\store\tokens.dat
 Reads from:
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
WindowsBackup%4ActionCenter.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
NetworkAccessProtection%4WHC.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows
Defender%4WHC.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
Scheduled%40perational.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Reads from:
TaskScheduler%4Maintenance.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Control
Panel%40perational.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-
 Reads from:
Notifications%4ActionCenter.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-
Core%4WHC.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-
  Reads from:
ConnectedAccountState%4ActionCenter.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
UserPnp%4ActionCenter.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-
 Reads from:
ManagementAgent%4WHC.evtx
                         C:\Windows\System32\spp\store\data.dat.tmp
 Deletes:
```

#### **Network Events**

Creates kev:

DNS query:	WORKGROUP
DNS query:	MSBROWSE
DNS query:	WORKGROUP
DNS query:	WPAD
Connects to:	10.74.1.255:138
Connects to:	10.74.1.255:137
Sends data to:	10.74.1.255:138
Sends data to:	10.74.1.255:137
Receives data from:	10.74.1.100:138
Receives data from:	10.74.1.100:137

Windows Registry Events		
Creates key:	<pre>HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-</pre>	
linklocal\linklocal	L_ff00::%12/8	
Creates key:	<pre>HKCU\software\classes\local settings\muicache\13\52c64b7e</pre>	
Creates key:	<pre>HKCU\software\classes\local settings\muicache</pre>	
Creates key:	HKLM\software\classes	
Creates key:	<pre>HKLM\system\currentcontrolset\services\vss\diag\registry writer</pre>	
Creates key:	<pre>HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer</pre>	
Creates key:	<pre>HKLM\system\currentcontrolset\services\vss\diag\asr writer</pre>	
Creates key:	<pre>HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization</pre>	
writer		
Creates key:	<pre>HKLM\system\currentcontrolset\control\stillimage\trace</pre>	
Creates key:	HKLM\system	
Creates key:	HKLM\system\currentcontrolset	
Creates key:	HKLM\system\currentcontrolset\control	

HKLM\svstem\currentcontrolset\control\stillimage

```
Creates key:
                           HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll
                           HKLM\system\currentcontrolset\services\nativewifip\parameters
 Creates key:
                           HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters
 Creates key:
 Creates key:
                           HKLM\system\currentcontrolset\services\nativewifip
                           HKLM\system\currentcontrolset\services\ndisuio
 Creates key:
                           HKLM\software\microsoft\windows nt\currentversion\networklist\nla\cache
 Creates kev:
 Creates key:
                           HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet
 Creates key:
                           HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet\
 Creates key:
                           HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant\store
 Creates key:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
 Creates key:
                           HKLM\system\wpa
                           HKLM\software\microsoft\security center\svc\vol
 Creates kev:
 Creates key:
                           HKLM\software\microsoft\security center
 Creates key:
                           HKLM\software\microsoft\security center\svc
 Creates key:
                           HKLM\software\microsoft\wbem\cimom
 Creates kev:
                           HKLM\software
 Creates key:
                           HKLM\software\microsoft
 Creates key:
                           HKLM\software\microsoft\wbem
 Creates key:
                           HKLM\system\currentcontrolset\services\sharedaccess\epoch
 Creates key:
                           {\tt HKLM \setminus software \setminus microsoft \setminus security \ center \setminus monitoring}
 Creates key:
                           HKLM\software\microsoft\windows\currentversion\policies\system
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34
 Creates key:
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
 Creates kev:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100
 Creates key:
                           HKCU\software\microsoft\windows\windows error reporting
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc\}.check.0
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\startupnotify
 Creates key:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
 Creates key:
center \verb|\providers| eventlog \verb|\final {01979c6a-42fa-414c-b8aa-eee2c8202018} |
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center \verb|\providers| eventlog \verb|\{dab69a6a-4d2a-4d44-94bf-e0091898c881\}| 
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
 Creates key:
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017\}.check.800
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{134ea407-755d-4a93-b8a6-f290cd155023}.check.8001
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
 Creates key:
center \verb|\providers| eventlog \verb|\c4efc9bb-2570-4821-8923-1bad317d2d4b| |
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key
center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
 Creates key:
center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
```

Creates key:  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action$ 

center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100

HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver] Deletes value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}[dhcpnameserver]

 $\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} system \end{tabular} \begin{tabular}{ll} LKLM \end{tabular} system \end{tabular} and \end{tabular} in the label{tabular} and \end{tabular} system \end{tabular} \begin{tabular}{ll} LKLM \end{tabular} system \end{tabular} \begin{tabular}{ll} LKLM \end{tabular} system \end{tabular} system \end{tabular} system \end{tabular} system \end{tabular} \begin{tabular}{ll} LKLM \end{tabular} system \end{tabular}$ Deletes value:

Deletes value:

55779daa70e9}[dhcpdomain]

Deletes value:

HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip\_{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserverlist]

Deletes value:

55779daa70e9}[dhcpsubnetmaskopt]

Deletes value:

55779daa70e9}[dhcpdefaultgateway]

HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid] Deletes value:

Deletes value:

 $HKLM \label{lem:hklm} Which is a substitution of the state of the st$ 

87b7-55779daa70e9}[dhcpnetbiosoptions]

Opens key:  ${\tt HKLM \backslash software \backslash microsoft \backslash wow64}$ 

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key:

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key:

Opens kev: HKLM\software\policies\microsoft\mui\settings

HKCU\software\policies\microsoft\control panel\desktop Opens key:

Opens kev: HKCU\control panel\desktop\languageconfiguration

HKCU\control panel\desktop Opens key:

Opens key:  ${\tt HKCU \backslash control\ panel \backslash desktop \backslash muicached}$ 

Opens key:  ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus side by side}$ Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\system\currentcontrolset\control\error message instrument\ HKLM\system\currentcontrolset\control\error message instrument Opens key: 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\system\currentcontrolset\control\cmf\config

Opens kev: 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:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ console\+ true type font$ Opens key:  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} console \end{tabular} co$ 

Opens key: HKCU\console Opens key: HKCU\console\

Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens key: HKLM\software\microsoft\sqmclient\windows

Opens kev: HKLM\svstem\currentcontrolset\control\nls\sorting\ids Opens key: HKLM\system\currentcontrolset\control\session manager  ${\tt HKCU\console\%} systemroot \verb§\_temp\_toggleservice32.exe$ Opens kev: Opens key:  $HKCU \verb|\console|| % system root % temp \verb|\toggleservice32.exe|| \\$ Opens key:  ${\tt HKLM \ } system \verb|\ current control \ set \verb|\ control \ | nls \verb|\ custom \ locale \\$ Opens key:  ${\tt HKLM \ } system \verb|\ current control \ | \ lextended locale$ 

Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts HKLM\system\currentcontrolset\control\nls\language groups Opens key:

Opens key: Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \direct manipulation \end{tabular}$ 

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:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \configuration \\ \begin{tabular}{ll} HKLM \end{tabular} system \configuration \\ \begin{tabular}{ll} HKLM \end{tabular} system \configuration \\ \begin{tabular}{ll} HKLM \end{tabular} system \e$ 

Opens key: HKLM\software\microsoft\ctf\

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the$ Opens key: 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 HKLM\system\currentcontrolset\control\nls\language Opens kev: Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key:  $HKLM \verb|\system| current control current control current control current control current control current control current current control current current control current current control current c$ 

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings Opens key:  $HKLM \verb|\system| current control current control current control current control current control current control current current control current control current control current control current control current current control current current current control current curr$ 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

HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file Opens key:

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

HKLM\system\setup Opens key:

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\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: 

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:  $HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\ \ in procserver 32$ Opens key:  $HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\nprochandler32$ Opens key:  $HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\nprochandler$ 

Opens key: HKLM\system\currentcontrolset\control\mui\settings

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

HKLM\software\policies\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography Opens kev:  ${\tt HKLM \cooptware \microsoft \cooptagraphy \cooptagraph$ Opens key:

HKCR\interface\{00000134-0000-0000-c000-000000000046} Opens kev:

HKCR\interface\{00000134-0000-0000-0000-00000000046}\proxystubclsid32 Opens key:

Opens key: HKLM\software\microsoft\rpc\extensions

Opens key:  $HKLM \ software \ microsoft \ windows runtime \ clsid \ \{f8ade1d3-49df-4b75-9005-64000\} \ description \ descript$ 

ef9508e6a337}

Opens key:  $HKCR\activatable classes \verb|\clsid|{f8} ade 1d3-49df-4b75-9005-ef9508e6a337{} ade 1d3-49df-4b75-9005-ef9508e6a356{} ade 1d3-49df-4b75-9005-ef9508e6a56{} ade 1d3-49df-4b75-9005-ef9508e608{} ade 1d3-49df-4b75-9006-ef9508{} ade 1d3-49df-4b75-9006-ef9508{} ade 1d$ 

HKCR\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337} Opens key: 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}

 $HKCR \ activatable classes \ \ clsid \ \ \{3ceb5509-c1cd-432f-9d8f-65d1e286aa80\}$ Opens kev:

Opens key: HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80} Opens kev:

 $HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{3ceb5509 - c1cd - 432f - 9d8f - 65d1e286aa80\}$ Opens key:  $HKLM \ software \ microsoft \ windows runtime \ clsid \ \{7b3181a0-c92f-4567-b0fa-b0fa-b181a0-c92f-4567-b0fa-b181a0-c92f-567-b0fa-b181a0-c92f-567-b0fa-b181a0-c92f-567-b0fa-b181a0-c92f-567-b0fa-b181a0-c92f-567-b0fa-b181a0-c92f-567-b0fa-b181a0$ 

cd9a10ecd7d1}

Opens key:  $HKCR \ activatable classes \ \ clsid \ \ \{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1\}$ 

Opens key: HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1} Opens key:

 $HKCR \setminus wow 6432 \\ node \\ clsid \\ \{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1\} \\$ Opens kev:

c117c14c429e}

Opens key: HKCR\activatableclasses\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}

HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e} Opens kev:

HKCR\wow6432node\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e} Opens key:

Opens key:

920843d40be5}

 $HKCR \ activatable classes \ \ clsid \ \ \{bbb36f15-408d-4056-8c27-920843d40be5\}$ Opens key:

HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5} Opens key:

Opens key:  $HKCR \ wow 6432 node \ clsid \ \{bbb 36f15-408d-4056-8c27-920843d40be5\}$ 

Opens key  $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{6f9942c9 - c1b1 - 4ab5 - 93da - based \setminus \{6f9942c9 - c1b1 - 4ab5 - 4ab5 - 4ab5 - 4ab5 - based \setminus \{6f9942c9 - c1b1 - 4ab5 - 4ab5 - 4ab5 - 4ab5 - based \setminus \{6f9942c9 - based - based \setminus \{6f9942c9 - based - based - based \setminus \{6f9942c9 - based - based - based \setminus \{6f9942c9 - based - based - based - based - based \setminus \{6f9942c9 - based - ba$ 

6058991dc8f3}

 $HKCR \ activatable classes \ \ clsid \ \ \{6f9942c9-c1b1-4ab5-93da-6058991dc8f3\}$ Opens key:

HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3} Opens key: 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}  $HKCR \setminus \{bc9b54ab-7883-4c13-909f-033d03267990\} \\$ Opens key:

Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{6e590d61 - f6bc - 4dad - ac21 - f6bc - f6$ 

7dc40d304059}

Opens key:  $HKCR \land activatable classes \land clsid \land \{6e590d61-f6bc-4dad-ac21-7dc40d304059\}$ 

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 HKLM\software\microsoft\msdtc\tracing\output Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc

HKLM\software\microsoft\msdtc Opens key:

Opens key: HKCR\cid.local

HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1 Opens key:

Opens key: Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\svcid

Opens key: HKCR\svcid.local

HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464 Opens key:

```
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
                                                                                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol
      Opens key:
      Opens key:
                                                                                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint
      Opens key:
                                                                                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties
                                                                                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties\log
      Opens key:
                                                                                           HKCR\cid.local\15546232-d044-45d4-88a8-
     Opens kev:
Ob84583f2fe1\customproperties\log\size
      Opens key:
                                                                                           HKLM\software\microsoft\msdtc\mtxoci
      Opens key:
                                                                                           HKLM\software\microsoft\msdtc\security
                                                                                           HKLM\software\microsoft\windows nt\currentversion\asr\restoresession
     Opens key:
      Opens key:
                                                                                           HKCR\cid.local\15546232-d044-45d4-88a8-
Ob84583f2fe1\customproperties\log\path
                                                                                           HKLM\software\microsoft\windows
      Opens key:
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
                                                                                           HKLM\software\microsoft\windows
      Opens kev:
nt\currentversion\tracing\msdtc\modules\transaction_transitions
                                                                                           HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed
      Opens key:
      Opens key:
                                                                                           HKLM\software\microsoft\windows nt\currentversion
      Opens key:
                                                                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac
      Opens key:
                                                                                           HKCR \verb|\cid.local| 4452c425-ad2f-4cde-b895-734b166ac4ac \verb|\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
                                                                                           HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
      Opens key:
      Opens key:
                                                                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\protocol
                                                                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint
      Opens key:
      Opens kev:
                                                                                           HKCU\control panel\international
                                                                                           HKLM\software\microsoft\rpc\securityservice
      Opens key:
      Opens kev:
                                                                                           HKLM\svstem\currentcontrolset\control\securityproviders
                                                                                           {\tt HKLM \ } system \verb|\ current control \ \\ lsa \verb|\ sspicache| \\
     Opens key:
      Opens key:
                                                                                           Opens key:
                                                                                           {\tt HKLM} \ system \verb|\currentcontrolset| control \verb|\securityproviders| saslprofiles \\
      Opens key:
                                                                                           HKCR \verb|\| cid.local \verb|\| 4452c425-ad2f-4cde-b895-734b166ac4ac \verb|\| customproperties | additional 
      Opens key:
                                                                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties\dac
                                                                                           HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc
      Opens key:
      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
                                                                                           HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid
      Opens key:
      Opens kev:
                                                                                           HKLM\svstem\currentcontrolset\control\lsa\accessproviders
      Opens key:
                                                                                           HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
      Opens kev:
                                                                                           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:
                                                                                           b913c40c9cd4}
      Opens key:
                                                                                           HKCR\activatableclasses\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
      Opens key:
                                                                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
      Opens kev:
                                                                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
                                                                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
     Opens key:
                                                                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
      Opens kev:
                                                                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
      Opens key:
      Opens key:
                                                                                           {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  key iso |
     Opens key:
                                                                                           HKLM\system\currentcontrolset\services\eaphost
      Opens key:
                                                                                           HKLM\software\policies\microsoft\windows nt\reliability
      Opens key:
                                                                                           HKLM\hardware\description\system\centralprocessor\0
      Opens key:
                                                                                           HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
appxdeploymentserver/operational
      Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
appxdeploymentserver/operational
      Opens key
                                                                                           \label{lem:hklm} \verb+Kklm \system \current control set \services \
networkprofile/operational
      Opens key:
HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv
networkprofile/operational
                                                                                          \label{lem:hklmsystem} \\ \text{HKLM} \\ \text{system} \\ \text{current} \\ \text{controlset} \\ \text{services} \\ \text{eventlog} \\ \text{microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-windows-microsoft-wi
     Opens key:
kernel-storemgr/operational
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - kernel-leave \ microsoft \ - windows \ - kernel-leave \
storemgr/operational
     Opens key:
                                                                                           HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
devicesetupmanager/operational
     Opens kev:
devicesetupmanager/operational
                                                                                           {\tt HKLM} \ system \verb|\currentcontrolset\ services\ | windows-leventlog \verb|\microsoft-windows-leventlog | windows-leventlog | w
      Opens key
userpnp/deviceinstall
      Opens key:
HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv
userpnp/deviceinstall
      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
                                             HKLM\software\microsoft\windows\currentversion
   Opens key:
   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 kev:
                                             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
                                             HKU\.default\software\microsoft\windows nt\currentversion
   Opens key:
   Opens key:
                                             HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
                                             HKLM\software\microsoft\windows nt\currentversion\appcompatflags
   Opens kev:
  Opens key:
                                             HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\ui0detect.exe
                                             HKU\.default\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
   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
                                             HKU\.default\control panel\desktop\muicached
   Opens key:
  Opens key:
                                             HKLM\system\currentcontrolset\services\sharedaccess
   Opens key:
                                             HKLM\system\currentcontrolset\services\sharedaccess\startoverride
                                             HKLM\software\microsoft\windows\currentversion\winevt
  Opens key:
                                             HKLM\software\microsoft\windows\currentversion\winevt\publishers
   Opens kev:
  Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{54849625-5478-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4964-a5ba-4964-a5ba-4994-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-496-a5b
3e3b0328c30d}
   Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{555908d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a6d7-4695-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-6660-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-1648d1-a606-8e1e-16
26931d2012f4}
  Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-
26931d2012f4}\channelreferences
   Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-
26931d2012f4}\channelreferences\0
                                             HKLM\system\currentcontrolset\services\eventlog\system\service control
   Opens key:
manager
   Opens kev:
                                             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 kev:
                                             HKLM\svstem\currentcontrolset\services\bits
                                             HKLM\system\currentcontrolset\services\bthserv
  Opens key:
   Opens kev:
                                             HKLM\system\currentcontrolset\services\cscservice
  Opens key:
                                             HKLM\system\currentcontrolset\services\deviceassociationservice
   Opens key:
                                             {\tt HKLM \ } system \verb| current control set \verb| services \verb| dns cache \\
  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\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 kev:
                                             HKLM\system\currentcontrolset\services\homegroupprovider
   Opens kev:
                                             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\peerdistsyc
  Opens key:
                                             HKLM\system\currentcontrolset\services\pla
   Opens key:
                                             HKLM\system\currentcontrolset\services\pnrpautoreg
                                             HKLM\system\currentcontrolset\services\printnotify
   Opens key:
   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\storsyc
 Opens kev:
                      HKLM\svstem\currentcontrolset\services\svsvc
 Opens key:
                      HKLM\system\currentcontrolset\services\tabletinputservice
 Opens kev:
                      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\svstem\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:
                      {\tt HKLM \backslash system \backslash current control set \backslash services \backslash wdisystem host}
 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\svstem\currentcontrolset\services\wlansvc
 Opens key:
                      HKLM\system\currentcontrolset\services\wlidsvc
 Opens kev:
                      HKLM\svstem\currentcontrolset\services\wpcsvc
 Opens key:
                      HKLM\system\currentcontrolset\services\wscsvc
 Opens kev:
                      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
                      HKU\s-1-5-19\volatile environment\0
 Opens kev:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
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
                      HKLM\software\microsoft\windows nt\currentversion\svchost
 Opens kev:
 Opens key:
                      HKLM\software\microsoft\windows
nt\currentversion\svchost\localservicepeernet
 Opens kev:
HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile
 Opens kev:
                      HKLM\svstem\currentcontrolset\services
 Opens key:
                      HKLM \setminus system \setminus current control set \setminus services \setminus p2pimsvc \setminus parameters
 Opens key:
                      \label{lem:hammon} \mbox{HKLM\software\mbox{$\mbox{$\mbox{microsoft\windows}$} nt\current\version\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
                      HKLM\system\currentcontrolset\services\pnrpsvc\parameters
 Opens key:
 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 kev:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9
 Opens key:
Opens key:
Opens kev:
Opens key:
Opens kev:
Opens key:
Opens key:
Opens key:
```

Opens key:

```
Opens key
Opens key:
Opens kev:
Opens key:
Opens key:
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries 64
  Opens key:
Opens kev:
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\0000000000004
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:
  Opens key:
                                 \label{lem:hklmsystem} \verb|HKLM\| system \verb| current control set \verb| services \verb| tcpip \verb| parameters \verb| winsock | system \verb| system \verb| current control set \verb| services \verb| tcpip \verb| parameters \verb| winsock | system \verb| system s
  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
                                 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
  Opens kev:
806e6f6e69633
  Opens key:
25b8d56dd1d8}
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
  Opens kev:
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 kev:
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 kev:
                                 HKLM\software\policies\microsoft\peernet\pnrp\ipv6-linklocal
  Opens key:
                                 HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal
  Opens kev:
                                 HKU\
                                 HKLM\system\currentcontrolset\services\crypt32
  Opens key:
  Opens kev:
                                 {\tt HKLM \ } software \verb|\ microsoft \ \\ cryptography \verb|\ oid \ \\
  Opens key:
                                 Opens key:
                                 {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \\
0\certdllopenstoreprov
  Opens key:
                                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
                                 {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ oid \verb|\ encoding type \\
  Opens key:
0\certdllopenstoreprov\ldap
  Opens key:
                                 HKLM\software\microsoft\cryptography\oid\encodingtype 1
  Opens key:
                                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
                                 HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
0\cryptdlldecodeobjectex
  Opens key:
                                 {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
1\cryptdlldecodeobjectex
  Opens key:
                                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
  Opens key:
                                 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
  Opens kev:
                                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
                                 HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
  Opens kev:
                                 {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \\
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 \verb|\software\m| icrosoft \verb|\cryptography\deshashsession| keybackward
  Opens key:
                                     HKLM\system\currentcontrolset\services\plugplay
  Opens key:
                                     HKLM\system\currentcontrolset\services\plugplay\startoverride
  Opens key:
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens kev:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7
                                     HKLM\system\currentcontrolset\control\mui\stringcachesettings
  Opens kev:
                                     HKCU \setminus software \setminus classes \setminus local\ settings \setminus muicache \setminus 13 \setminus 52c64b7e
  Opens key:
  Opens kev:
                                     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:
                                     {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ oid \verb|\ encoding type \\
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7
                                     {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\
  Opens key:
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
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
0\cryptdllencodepublickeyandparameters
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
{\tt 1} \verb| cryptdllencodepublickey| and parameters
  Opens key:
                                     {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
0\cryptdllencodeobjectex
  Opens key:
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex
                                    Opens key:
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
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens kev:
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.11
  Opens kev:
                                     {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \\
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.12
  Opens kev:
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.2
  Opens key:
                                     {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \\
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.3
                                     {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.4
  Opens key:
                                     HKLM\system\currentcontrolset\services\spooler
  Opens key:
                                     HKLM\system\currentcontrolset\services\spooler\startoverride
  Opens key:
                                     HKLM\system\currentcontrolset\services\http
  Opens kev:
                                     HKLM\system\currentcontrolset\services\dcomlaunch
  Opens key:
                                     HKLM\system\currentcontrolset\services\rpceptmapper
  Opens kev:
                                     HKLM\system\currentcontrolset\services\rpcss
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe
  Opens key:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage 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\svstem\currentcontrolset\services\rpcss\startoverride
  Opens key:
                                     HKLM\system\currentcontrolset\control\print
  Opens kev:
                                     HKCR\clsid
                                     HKLM\software\policies\microsoft\windows nt\printers
  Opens key:
  Opens kev:
                                     HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:
Opens key:
                                     \label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{}\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{
  Opens key:
                                     HKLM\software\microsoft\telemetryclient\throttlestore\sqm
  Opens key:
                                     HKLM\software\microsoft\telemetryclient\throttlestore
                                     HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
  Opens key:
  Opens key:
                                     HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
  Opens key:
                                     HKLM\software\microsoft\telemetryclient\samplestore\sqm
  Opens key:
HKLM \setminus software \setminus microsoft \setminus telemetry client \setminus throttlestore \setminus sqm \setminus windows \setminus winsqm8 \setminus 13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
  Opens kev:
HKLM \ software \ microsoft \ telemetry client \ throttlestore \ sqm \ windows \ winsqm 8 \ 13238784
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
  Opens key:
                                     HKLM\system\currentcontrolset\services\seclogon\startoverride
                                     HKLM\system\currentcontrolset\services\sens
  Opens key:
  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
                                     HKLM\system\currentcontrolset\services\schedule
  Opens kev:
  Opens key:
                                     HKLM\system\currentcontrolset\services\schedule\startoyerride
  Opens key:
                                     HKLM\svstem\currentcontrolset\services\lmhosts
                                     HKLM\system\currentcontrolset\services\lmhosts\parameters
  Opens key:
  Opens key:
                                     HKLM\system\currentcontrolset\services\lmhosts\startoverride
  Opens key:
                                     {\tt HKLM \ } system \verb|\ current control \ \\ diagnostics \verb|\ performance| \\
  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
                                                                                       {\tt HKLM \backslash system \backslash current control set \backslash services \backslash vss \backslash vss access control}
      Opens key:
     Opens kev:
                                                                                       HKCR\appid\vssvc.exe
                                                                                       Opens key:
de0991ff0623}
      Opens key:
                                                                                       HKCR \ activatable classes \ \ 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
                                                                                       HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
      Opens key:
      Opens key:
                                                                                       HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler
     Opens key:
                                                                                       6c6d4570e40f}
      Opens key:
                                                                                       HKCR\activatableclasses\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
      Opens key:
                                                                                       HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
                                                                                       \label{locality} $$ HKCR\clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \times \clid_{0b5a2c52-3eb9-470a-96e2-6c6d4570
     Opens key:
      Opens key:
                                                                                       \label{lem:hkcr} $$ HKCR\clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \in \clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} $$ inprocessor of the context of the
      Opens key:
                                                                                       \label{lem:hkcr} $$HKCR\clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler 32 $$
      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 \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{4e14fba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e24ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4b
00c04fbbb345}
                                                                                       HKCR\activatableclasses\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
      Opens key:
      Opens key:
                                                                                       HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
                                                                                       HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
     Opens key:
                                                                                       HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32
     Opens kev:
                                                                                       \label{local-eq:hkcr} \begin{tabular}{ll} HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\end{tabular} \label{line-eq:hkcr} $$ in prochamdler 32. $$ in prochamble $$ in pro
     Opens key:
      Opens key:
                                                                                       HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\ \ in prochandler
     Opens key:
                                                                                       HKLM \ software \ microsoft \ windows runtime \ clsid \ \{1be1f766-5536-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d1-b726-11d
00c04fb926af}
      Opens key:
                                                                                       HKCR \ activatable classes \ \ \{1be1f766-5536-11d1-b726-00c04fb926af\}
                                                                                       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:
      Opens key:
                                                                                       HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
                                                                                       HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler
      Opens key:
      Opens key:
                                                                                       HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
     Opens key:
                                                                                       HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32
                                                                                       HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{64b8f404 - a4ae - 11d1 - b7b6 - a4ae - a4
     Opens key:
00c04fb926af}
      Opens key:
                                                                                       HKCR \land activatable classes \land clsid \land \{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}\
      Opens key:
                                                                                       HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\ \ in prochandler 32
      Opens key:
                                                                                       HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\nprochandler
     Opens key:
                                                                                       HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger
                                                                                       HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}
      Opens key:
      Opens key:
                                                                                       HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
     Opens key:
                                                                                       HKCR\interface\{00000100-0000-0000-c000-00000000046}
                                                                                       Opens key:
     Opens key:
                                                                                       Opens key:
                                                                                       HKCR\ interface \ \{609b9555-4fb6-11d1-9971-00c04fbbb345\} \ proxystubclsid32
      Opens key:
                                                                                       HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{7542e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-14400-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-79c7-1440-7
0080c7d771bf}
      Opens key:
                                                                                       HKCR\activatableclasses\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
      Opens key:
                                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
                                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
      Opens key:
                                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32
     Opens key:
      Opens key:
                                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler32
     Opens kev:
                                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler
                                                                                       HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}
     Opens kev:
                                                                                       HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345\}\proxystubclsid32
     Opens key:
     Opens key:
                                                                                       HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
      Opens key:
                                                                                       \label{lem:hklm} \verb+Kklm \system \current control set \services \vss \diag \asr writer
      Opens key:
                                                                                       HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization
writer
      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\parameters
     Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus certificates \setminus 2bd63d28d7bcd0e251195aeb519243c13142ebc3
     Opens key:
Opens kev:
Opens key:
                                                                                       HKLM\system\currentcontrolset\services\eventlog\application\vss
      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\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-
  a3cc-00a0c9223196}
          Opens key:
                                                                                                                                HKLM\software\microsoft\windows\currentversion\audio
                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\svchost\wersvcgroup
          Opens kev:
          Opens key:
                                                                                                                                HKU\.default\control panel\international
         Opens key:
                                                                                                                                HKLM\system\currentcontrolset\services\wersvc\parameters
                                                                                                                                HKLM\software\microsoft\windows\windows error reporting
          Opens key:
         Opens kev:
                                                                                                                                HKLM\system\currentcontrolset\services\mpssvc\startoverride
          Opens key:
 HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{6bba3851-2c7e-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f
 31e5afd029e3}
         Opens key:
                                                                                                                                HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
  diagnosis-dps/debug
          Opens kev:
 HKLM \ software \ microsoft \ windows \ -current version \ winevt \ channels \ microsoft -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis \ -diagn
 dps/debug
         Opens key
                                                                                                                                HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
 diagnosis-dps/operational
         Opens key:
 HKLM \setminus software \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - diagnosis - windows - wind
 dps/operational
          Opens key:
                                                                                                                                \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ event \+ log \+ microsoft - windows - log \+ microsoft - w
 diagnosis-dps/analytic
          Opens key:
  HKLM \label{lem:hkklm} HKLM \label{lem:hkklm} HKLM \label{lem:hkklm} Windows \label{lem:hkklm} \label{lem:hkklm} Limit \label{lem:hkklm} HKLM \label{lem:hkklm} \label{lem:hkklm} \label{lem:hkklm} HKLM \label{lem:hkklm} \label{
 dps/analytic
          Opens kev:
 HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-
 622caee05b0a}
                                                                                                                                \label{lem:hklm} \verb+Kklm \system \current control set \services \
         Opens key:
 diagnostics-performance/operational
         Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
 performance/operational
          Opens key:
                                                                                                                                {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ current control set \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ current control set \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ current control set \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ current control set \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \verb|\ microsoft-windows-def}| and the system \verb|\ services \verb|\ eventlog \ even
 diagnostics-performance/diagnostic
          Opens key:
 HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic
          Opens key:
                                                                                                                                HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
 diagnostics-performance/diagnostic/loopback
         Opens kev:
 \label{tware} \begin{tabular}{ll} HKLM \label{tware} \b
 performance/diagnostic/loopback
                                                                                                                                HKLM\system\currentcontrolset\services\stisvc
          Opens key:
          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 \cdot appid \cdot \{a1f4e726-8cf1-11d1-bf92-0060081ed811\}
                                                                                                                                HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{a1f4e726-8cf1-11d1-bf92-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-14e82-1
          Opens kev:
 0060081ed811}
                                                                                                                                HKCR\activatableclasses\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
          Opens key:
                                                                                                                                HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
          Opens kev:
                                                                                                                                HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\treatas
         Opens key:
                                                                                                                                HKCR \verb|\clsid|{a1f4e726-8cf1-11d1-bf92-0060081ed811} \verb|\inprocserver32|
          Opens kev:
          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:
                                                                                                                                8ec92617e599}
          Opens key:
                                                                                                                                HKCR\activatableclasses\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
                                                                                                                                HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
          Opens kev:
          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 \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{a1e75357 - 881a - 419e - 83e2 - 419e - 83
  bb16db197c68}
           Opens key:
                                                                                                                                HKCR \land activatable classes \land clsid \land \{a1e75357-881a-419e-83e2-bb16db197c68\}
          Opens key:
                                                                                                                                HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
                                                                                                                                HKCR\wow6432node\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
          Opens key:
          Opens key:
                                                                                                                                HKLM\system\currentcontrolset\control\stillimage\mscdevicelist
         Opens key:
                                                                                                                                HKLM\system\currentcontrolset\control\stillimage
          Opens key:
                                                                                                                                HKLM\system\currentcontrolset\control\stillimage\events
         Opens kev:
                                                                                                                                HKLM\system\currentcontrolset\control\stillimage\events\connected
         Opens key:
 6c15f82b5905}
          Opens key:
                                                                                                                                HKLM\system\currentcontrolset\control\stillimage\events\disconnected
          Opens key:
                                                                                                                                HKLM\system\currentcontrolset\control\stillimage\events\emailimage
         Opens key:
 759eb35cdf9a}
```

```
Opens key:
                                          HKLM\system\currentcontrolset\control\stillimage\events\faximage
   Opens key:
759eb35cdf9a}
  Opens key:
                                          HKLM\system\currentcontrolset\control\stillimage\events\printimage
  Opens kev:
759eb35cdf9a}
   Opens key:
                                          HKLM\system\currentcontrolset\control\stillimage\events\scanbutton
  Opens key:
783ce7a92f22}
   Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
   Opens kev:
HKLM \ system \ current control \ stillimage \ events \ scanbutton \ \{eabbd70d-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96
7105fd3b53b1}
  Opens key:
6c15f82b5905}
   Opens key:
                                          HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent
  Opens key:
                                          {\tt HKLM \ } system \verb|\ current control \ $tillimage \ $server settings \\
  Opens key:
                                          HKLM \verb|\system| current control set \verb|\services| \verb|\w32time| start over ride|
   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:
                                          Opens key:
                                          HKLM\system\currentcontrolset\services\wcmsvc
  Opens key:
                                          HKLM\system\currentcontrolset\services\ndisuio
  Opens key:
                                          HKLM\svstem\currentcontrolset\services\nativewifip
                                          HKLM\system\currentcontrolset\services\nativewifip\parameters
  Opens key:
  Opens kev:
                                          HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
                                          HKLM \ system \ current control \ etwork \ \{4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-11ce-bfc1-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e974-e325-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e976-e4d36e
  Opens key
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
  Opens key
Opens key:
                                          08002be10318}\0010
  Opens key:
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010\linkage
   Opens key:
                                          HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
  Opens key
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007
                                          HKLM\system\currentcontrolset\services\nnetsecl\parameters
  Opens key:
   Opens kev:
                                          HKLM\svstem\currentcontrolset\enum\root\ms ndiswanip\0000
                                          Opens key
08002be10318}\0005
  Opens key:
                                          08002be10318}\0007\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
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens key:
08002be10318}\0005\linkage
                                          HKLM\system\currentcontrolset\enum\root\ms pppoeminiport\0000
  Opens key:
   Opens key
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004
  Opens key:
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage
   Opens key:
                                          HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000
   Opens key:
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000
  Opens key:
                                          08002be10318}\0000\linkage
   Opens key:
                                          HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens kev:
08002be10318}\0003
                                          HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens kev:
08002be10318}\0003\linkage
   Opens key:
                                          {\tt HKLM \ } system \verb|\ current control set \verb|\ enum \verb|\ root \verb|\ * is a tap \verb|\ 0000 \\
  Opens key:
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011
   Opens key:
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage
   Opens kev:
                                          HKLM\svstem\currentcontrolset\enum\root\*teredo\0000
   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}\0012\linkage
                                          HKLM\system\currentcontrolset\enum\root\ms agilevpnminiport\0000
   Opens key:
  Opens kev:
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002
   Opens key
                                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage
   Opens key:
                                          HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000
   Opens key:
                                          HKLM\system\currentcontrolset\services\wlansvc\linkage
```

Opens key:

HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

```
08002be10318}\0001
                                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
           Opens key
08002be10318}\0001\linkage
          Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\control\wmi\security
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\wlansvc\parameters
                                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
         Opens key
08002be10318}
                                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
         Opens kev:
 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}\properties
          Opens key:
                                                                                                                                                 HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{fc5eeaf6-2001-11df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14df-adb9-14d
  f4ce462d9137}
                                                                                                                                                 HKCR \ activatable classes \ \ \ \{fc5 ee af6-2001-11 df-adb9-f4ce 462 d9137\}
          Opens kev:
                                                                                                                                                 HKCR\clsid\{fc5eeaf6-2001-11df-adb9-f4ce462d9137}
          Opens key:
          Opens key:
                                                                                                                                                 HKCR\clsid\{fc5eeaf6-2001-11df-adb9-f4ce462d9137}\ \ treat as
                                                                                                                                                 HKCR\clsid\{fc5eeaf6-2001-11df-adb9-f4ce462d9137}\ \ \ in procserver 32
         Opens key:
                                                                                                                                                 HKCR\clsid\{fc5eeaf6-2001-11df-adb9-f4ce462d9137}\inprochandler32
          Opens kev:
                                                                                                                                                 \label{local-equation} HKCR\clsid\fc5eeaf6-2001-11df-adb9-f4ce462d9137\\\label{local-equation-equation} HKCR\clsid\fc5eeaf6-2001-11df-adb9-f4ce462d9137\\\label{local-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation-equation
         Opens key:
         Opens key:
                                                                                                                                                 HKLM\software\microsoft\wcmsvc
         Opens key:
                                                                                                                                                 {\tt HKLM \setminus software \setminus microsoft \setminus wcmsvc \setminus subscription manager}
         Opens key:
                                                                                                                                                 {\tt HKLM \ } system \verb|\ current control \ \\ control \verb|\ cryptography \verb|\ providers \ \\
         Opens key:
                                                                                                                                                 Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus winevt \setminus publishers \setminus \{67d07935-283a-4791-8f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d
 fa9117f3e6f2}
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
wcmsvc/operational
         Opens kev:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind
wcmsvc/operational
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
wcmsvc/diagnostic
         Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind
wcmsvc/diagnostic
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-
 15ef97d4c7c3}
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
crypto-dpapi/operational
         Opens kev:
\label{thm:local_hammels} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} irrors of t-windows-crypto-particles \end{tabular} and the constraint \end{tabular} and the constraint \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} and the constraint \en
dpapi/operational
         Opens key:
                                                                                                                                                 crypto-dpapi/backupkeysvc
         Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-part \ windows \ - crypto-part \ windows \ - crypto-part \ - cr
dpapi/backupkeysvc
          Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
 crypto-dpapi/debug
         Opens key:
HKLM \ software \ microsoft-windows \ - crypto-winevt \ - channels \ - crypto-windows \
dpapi/debug
         Opens kev:
d5be7d52d6de}
         Opens key
                                                                                                                                                 {\tt HKLM} \ system \verb|\currentcontrolset\ services \verb|\eventlog\ microsoft-windows-wlan-def} \\
 autoconfig/operational
         Opens key:
HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-wlandard \ microsoft-windows \
autoconfig/operational
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-wlan-
autoconfig/diagnostic
         Opens key:
HKLM \verb|\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-wlandows \verb|\software\microsoft-windows\channels\microsoft-windows-wlandows \verb|\software\microsoft-windows\channels\microsoft-windows\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\c
autoconfig/diagnostic
         Opens key:
                                                                                                                                                 HKLM\software\policies\microsoft\windows\appcompat
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\tcpip\parameters
         Opens key:
Opens kev:
 HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{b5105d63-74c6-4dc1-
87b7-55779daa70e9}
          Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}\parameters\tcpip
         Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\netbt\adapters\{b5105d63-74c6-
 4dc1-87b7-55779daa70e9}
          Opens key:
                                                                                                                                                 HKLM\system\currentcontrolset\services\netbt\parameters
         Opens key:
                                                                                                                                                 HKCU\software\classes\applications\calc.exe
         Opens key:
                                                                                                                                                 HKCR\applications\calc.exe
                                                                                                                                                 HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
         Opens key:
                                                                                                                                                 HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
          Opens key:
         Opens key
                                                                                                                                                HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-
```

Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\policies\microsoft\windows\edgeui

4a431715d9a3}\proxystubclsid32

```
Opens key:
                                                      \label{localized} HKCU \setminus software \\ \\ classes \setminus interface \\ \\ \{92ca9dcd-5622-4bba-a805-5e9f541bd8c9\} \\ \\ \\ equivalent \\ \\ eq
   Opens key:
                                                      HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
   Opens key:
                                                      HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-
5e9f541bd8c9}\proxystubclsid32
   Opens key:
                                                      HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
                                                      HKLM\system\currentcontrolset\services\eventlog\system\browser
   Opens key:
                                                      HKLM\software\microsoft\ctf\knownclasses
   Opens key:
                                                      HKLM\system\currentcontrolset\services\sppsvc
   Opens key:
   Opens key:
                                                      HKU\s-1-5-20
                                                      \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/profilelist/s-1-5-20 \\
   Opens key:
   Opens key:
                                                      shell folders
   Opens key:
                                                      HKU\s-1-5-20\environment
   Opens key:
                                                      HKU\s-1-5-20\volatile environment
   Opens key:
                                                      HKU\s-1-5-20\volatile environment\0
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens kev:
options\sppsvc.exe
   Opens key:
                                                      HKLM\system\currentcontrolset\control\session manager\quota system\s-1-
5-20
   Opens kev:
                                                      HKCR\appid\sppsvc.exe
                                                      HKLM\system\currentcontrolset\services\eventlog\application\software
   Opens key:
protection platform service
   Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{e23b33b0-c8c9-472c-a5f9-microsoft\} \ windows \ version \ versio
f2bdfea0f156}
                                                      HKLM\software\microsoft\windows
    Opens key:
nt\currentversion\softwareprotectionplatform
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10
   Opens key:
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14
   Opens kev:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15
   Opens key:
   Opens kev:
                                                      HKLM\system\currentcontrolset\services\wsearch
   Opens key:
                                                      {\tt HKLM \backslash system \backslash current control set \backslash services \backslash wmpnetworksvc}
   Opens key:
                                                      {\tt HKLM \ } system \verb| current control set \verb| services \verb| winmgmt | \\
   Opens key:
                                                      HKLM\system\currentcontrolset\services\wscsvc\parameters
   Opens key:
                                                      HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-16
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18
   Opens key:
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2
   Opens key:
                                                      HKLM\software\microsoft\security center\svc\vol
                                                      HKLM\software\microsoft\security center\svc
   Opens key:
                                                      HKLM\software\microsoft\windowsruntime\clsid\{4590f811-1d3a-11d0-891f-
   Opens kev:
00aa004b2e24}
                                                      HKCR \land activatable classes \land clsid \land \{4590f811-1d3a-11d0-891f-00aa004b2e24\}
   Opens kev:
                                                      HKCR \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\}
   Opens key:
   Opens key:
                                                      HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
   Opens key:
                                                      HKCR \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \ \ inprocserver 32
   Opens key:
                                                      \label{lem:hkcr} $$HKCR\clsid_{4590f811-1d3a-11d0-891f-00aa004b2e24}\in Clsid_{4590f811-1d3a-11d0-891f-00aa004b2e24} in prochandler 32 $$HKCR_clsid_{4590f811-1d3a-11d0-891f-00aa004b2e24} $$
   Opens key:
                                                      HKLM\software\policies\microsoft\system\dnsclient
   Opens kev:
   Opens key:
                                                      HKLM\software\microsoft\windowsruntime\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}
                                                      HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens kev:
                                                      HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
                                                      HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
   Opens kev:
                                                      HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
   Opens key:
   Opens key:
                                                      HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\tinprochandler 32
   Opens key:
                                                      HKCR \ clsid \ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \ \ in prochandler
   Opens key:
                                                      HKCR \ clsid \ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \ localser ver 32
   Opens key:
                                                      HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
                                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20
                                                      HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
   Opens key:
                                                      HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\elevation
   Opens key:
   Opens key:
                                                      HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
                                                      HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
                                                      HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
   Opens key
00c04fb68820}\localserver32
   Opens key
                                                      00c04fb68820}\localserver
   Opens key:
                                                      \label{lem:hkcrwow6432} HKCR\wow6432 node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\elevation} \\
   Opens key:
                                                      HKCR \setminus unmarshalers \setminus system \setminus \{00000339-0000-0000-c000-000000000046\}
   Opens key:
                                                      HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
   Opens key:
                                                      HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11cf-884d-11c
   Opens key:
00aa004b2e24}
   Opens key:
                                                      HKCR\activatableclasses\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
   Opens key:
                                                      HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
   Opens key:
                                                      HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
                                                      HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
   Opens key:
                                                      HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
   Opens key:
                                                      Opens key:
                                                      HKCR\ interface \ \{d4781cd6-e5d3-44df-ad94-930efe48a887\}
   Opens key:
   Opens key:
                                                      HKCR \ interface \ \{d4781cd6-e5d3-44df-ad94-930efe48a887\} \ proxystubclsid32
   Opens key:
                                                      HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
    Opens key:
                                                      Opens key:
```

```
ce99a996d9ea}
      Opens key:
                                                                                HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
     Opens key:
                                                                                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
     Opens key:
                                                                                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
     Opens key:
                                                                                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21
     Opens key:
                                                                                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32
     Opens key:
                                                                                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler
     Opens key:
                                                                                HKLM\software\microsoft\wbem\cimom
     Opens key:
                                                                                HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}
     Opens key:
                                                                                HKCR \ activatable classes \ \ clsid \ \ \{e7d35cfa-348b-485e-b524-252725d697ca\}
     Opens key:
                                                                                HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
     Opens key:
                                                                                HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\treatas
     Opens key:
                                                                                HKCR\clsid\e7d35cfa-348b-485e-b524-252725d697ca\\\label{e7d35cfa-348b-485e-b524-252725d697ca}\label{e7d35cfa-348b-485e-b524-252725d697ca}
     Opens key:
                                                                                HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler32
                                                                                HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler
     Opens key:
     Opens key:
                                                                                HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}
     Opens key:
                                                                                HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\proxystubclsid32
     Opens key:
                                                                                HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{71285c44-1dc0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5fb-14c0-11d2-b5f
00104b703efd}
                                                                                HKCR \ activatable classes \ \ \ \{71285c44-1dc0-11d2-b5fb-00104b703efd\}
     Opens key:
                                                                                HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}
     Opens key:
                                                                                HKCR \ clsid \ \{71285c44-1dc0-11d2-b5fb-00104b703efd\} \ treat as
     Opens key:
     Opens key:
                                                                                HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32
     Opens key:
                                                                                HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprochandler32
     Opens key:
                                                                                HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\ \ in prochandler
     Opens key:
     Opens key:
                                                                                HKCR\interface\{00020400-0000-0000-c000-00000000046}
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22
     Opens key:
     Opens key:
                                                                                HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\forward
     Opens key:
                                                                                HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\typelib
     Opens key:
                                                                                HKCR\interface\{027947e1-d731-11ce-a357-00000000001}
                                                                                HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32
     Opens key:
     Opens key:
                                                                                HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1cad8c-2dab-1b1
00104b703efd}
     Opens key:
                                                                                HKCR \ activatable classes \ \ \ \{1b1cad8c-2dab-11d2-b604-00104b703efd\}
     Opens key:
                                                                                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd\}
     Opens key:
                                                                                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
     Opens key:
                                                                                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\ \ inprocserver 32
                                                                                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
     Opens key:
                                                                                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler
     Opens key:
     Opens key:
                                                                                HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
     Opens key:
                                                                                HKCR\ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\}\ proxystubclsid 32
                                                                                HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
     Opens key:
                                                                                HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
     Opens kev:
     Opens key
                                                                                e02f0b373803}
                                                                                HKCR \ activatable classes \ \ \ \{bfe18e9c-6d87-4450-b37c-e02f0b373803\}
     Opens key:
     Opens kev:
                                                                                HKCR \verb|\clsid|{bfe} 18e9c-6d87-4450-b37c-e02f0b373803}
                                                                                \label{local-bound} $HKCR\clsid{bfe} 18e9c-6d87-4450-b37c-e02f0b373803} \treat as
     Opens key:
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24
     Opens key:
                                                                                HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25
     Opens key:
     Opens key:
                                                                                HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprochandler32
     Opens key:
                                                                                HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprochandler
     Opens key:
                                                                                HKLM\system\currentcontrolset\control\compression
     Opens kev:
                                                                                HKLM\software\microsoft\windows\currentversion\windowsupdate\trace
     Opens key
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} folder descriptions
     Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ expl
9d55-7b8e7f157091}
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28
     Opens kev:
     Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-explorer' \ 'f1b32785-6fba-4fcf-explore
9d55-7b8e7f157091}\propertybag
     Opens key:
                                                                               HKCU\software\microsoft\windows\currentversion\explorer
     Opens kev:
                                                                                \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \session in folding the lemma of t
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3
     Opens key:
                                                                                HKLM\software\policies\microsoft\windows\explorer
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32
     Opens key:
                                                                                HKCU\software\policies\microsoft\windows\explorer
     Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc
9afe-ea3317b67173}
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6
     Opens key:
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8
     Opens key:
                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9
     Opens key:
```

```
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc
9afe-ea3317b67173}\propertybag
      Opens key:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} known folders ettings
                                                                                                HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\misc
      Opens key:
      Opens kev:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\report
                                                                                               HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\setup
      Opens kev:
      Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\service
      Opens key:
                                                                                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} windows \begin{tabular}{ll} place \end{tabular} windows \beg
      Opens key:
                                                                                                HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\au
      Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\auclnt
                                                                                                HKLM \ software \ microsoft \ windows \ current version \ window supdate \ trace \ cltui
      Opens key:
                                                                                                HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cpl
      Opens kev:
      Opens key:
                                                                                                HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wuapp
      Opens key:
                                                                                                HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wuweb
      Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\dtastor
                                                                                                HKLM\software\microsoft\windows\currentyersion\windowsupdate\trace\cdm
      Opens key:
                                                                                                \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \label{lklmsoftware} \begi
      Opens key:
      Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus window supdate \setminus trace \setminus driver
      Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\comapi
      Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\parser
      Opens kev:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\handler
      Opens kev:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\eehndlr
      Opens kev:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus windows update \setminus trace \setminus dnldmgr
      Opens kev:
Opens key:
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wuredir
      Opens key:
```

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the local distribution of the local distribution$ 

Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\inv Opens kev: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\arp Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\trace Opens kev:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} window supdate \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lkm} \label{$ 

Opens kev:

 $HKLM \ software \ microsoft \ windows \ current version \ window supdate \ trace \ trace test threads$ 

Opens key:  $HKLM \ software \ \ icrosoft \ \ \ current version \ \ \ windows update \ \ trace \ \ perf,$ Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\ep Opens key:

HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wutask

Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\mowu

Opens key:

HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\rebootnotifv

Opens key:

 $\label{twindows} \verb|HKLM| software \verb|microsoft| windows \verb|currentversion| windows updates y sprepin progress$ Opens key: HKLM\software\policies\microsoft\windows\windowsupdate Opens key: HKLM\software\policies\microsoft\windows\windowsupdate\au

Opens key:  $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft| windows \end{tabular} update \end{tabular}$ Opens key:  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus windows update$ Opens key: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto

update\rebootrequired

Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-

3937643e37a3}

HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-Opens kev:

codeintegrity/operational

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} windows \end{tabular} irror soft-windows \end{tabular} and the local properties of the local propertie$ 

codeintegrity/operational

Opens kev:

4139-a9ba-be0bbbf5b74d\2fb92682-6599-42dc-ae13-bd2ca89bd11c

HKLM\system\currentcontrolset\services\eventlog\application\securitycenter

Opens key: HKLM\software\microsoft\windows\currentversion\policies\system Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-

codeintegrity/verbose

Opens kev:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

codeintegrity/verbose

Opens key: HKCU\software\microsoft\windows  $\verb|nt\currentversion\software| protection platform \verb|persistedts| rearmed| \\$ Opens key: HKCU\software\microsoft\windows

 $\verb|nt\currentversion\software| protection platform \verb|persisted system state| \\$ 

Opens key: HKLM\software\microsoft\windows

nt\currentversion\softwareprotectionplatform\plugins\modules

```
Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
 nt \verb|\currentversion| software protection platform \verb|\plugins| modules \verb|\179b8a65-b0f6-41d9-acea-12006ef9b32a| software protection platform \verb|\plugins| modules \verb|\179b8a65-b0f6-41d9-acea-12006ef9b32a| software protection platform \verb|\plugins| modules m
            Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb|`currentversion| software protection platform \verb| plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection platform | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the protection | plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| and the plugins | modules | c42d83ff-5958-4af4-a0dd-ba02fed39662| 
                                                                                                                                                                  HKLM\software\microsoft\windows
          Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects
                                                                                                                                                                  HKLM\software\microsoft\windows
          Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0
          Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
\verb| nt\current version \software protection platform \plugins \sobjects \mbox{\sc m/algorithm/bios/4.0}| \\
           Opens key
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/flags/1.0| | the following the following platform of the following platform
                                                                                                                                                                  HKLM\software\microsoft\windows
           Opens key:
Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0
          Opens key:
                                                                                                                                                                 HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/pkey/2005| | the following the following platform of the following platform
          Opens key:
                                                                                                                                                                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkev/2009
                                                                                                                                                                 HKLM\software\microsoft\windows
          Opens kev:
\verb|nt| current version \\| software protection platform \\| plugins \\| objects \\| msft:rm/algorithm/pkey/detection \\| plugins \\| objects \\| msft:rm/algorithm/pkey/detection \\| objects \\| objec
          Opens key:
                                                                                                                                                                 HKLM\software\microsoft\windows
 nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/vmd/1.0| | for the property of the property
                                                                                                                                                                  HKLM\software\microsoft\windows
           Opens key:
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/volume/1.0| and the protection platform objects ob
           Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform \verb|plugins\objects\mbox| msft: \verb|spp/action/create| process/1.0 | ms
          Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/action/kernel/1.0| |
                                                                                                                                                                  HKLM\software\microsoft\windows
          Opens kev:
\verb| nt\current version \software protection platform \verb| plugins \sobjects \scalebase | msft: spp/action/reeval/1.0| | msft:
          Opens kev:
                                                                                                                                                                  HKLM\software\microsoft\windows
Opens kev:
                                                                                                                                                                  HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0
           Opens key
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft:spp/apihandler/object/activedirectory publisher/1.0| and the province of the protection of the p
           Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/collector/global/1.0| | to the plugins \verb| objects | objects \verb| objects | objects \verb| objects | objects | objects | o
                                                                                                                                                                  HKLM\software\microsoft\windows
          Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0
                                                                                                                                                                 HKLM\software\microsoft\windows
          Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0
                                                                                                                                                                 HKLM\software\microsoft\windows
          Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0
          Opens key:
                                                                                                                                                                 HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition| payload handler/pkc/1.0 | like the platform of the pl
          Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft|: spp/license acquisition/payload handler/rac/1.0
                                                                                                                                                                  HKLM\software\microsoft\windows
           Opens key:
Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0
                                                                                                                                                                  HKLM\software\microsoft\windows
          Opens kev:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey
                                                                                                                                                                  HKLM\software\microsoft\windows
          Opens kev:
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft|: spp/task scheduler/1.0| and the subject of the subject of
          Opens kev:
                                                                                                                                                                  HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/volume/services/kms/1.0| | the first objects obje
          Opens key:
                                                                                                                                                                  HKLM\software\microsoft\windows
 nt \verb|\colored | holds | hold
                                                                                                                                                                  HKLM\software\microsoft\windows
           Opens key:
Opens key:
                                                                                                                                                                  HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
           Opens key:
                                                                                                                                                                  HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
                                                                                                                                                                  HKLM\software\microsoft\windows nt\currentversion\
           Opens key:
                                                                                                                                                                  HKLM\system\setup\status
           Opens kev:
                                                                                                                                                                  HKCU\software\microsoft\windows
          Opens key:
nt\currentversion\softwareprotectionplatform\reboot.sl brt commit
           Opens key
                                                                                                                                                                  HKLM \ system \ current control set \ enum \ acpi \ pnp0a03 \ \ 0
          Opens key
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00
           Opens key:
 HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08
                                                                                                                                                                  Opens key:
           Opens key:
                                                                                                                                                                  Opens key:
                                                                                                                                                                  HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0
           Opens key:
                                                                                                                                                                  HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0
           Opens key:
Opens key:
                                                                                                                                                                  Opens key:
           Opens key:
Opens key:
                                                                                                                                                                  \label{local-control} HKLM \ system \ current controls et \ enum \ pciide \ idechannel \ 4\&20064 fa 2\&0\&0 \ enum \ pciide \ idechannel \ below \ enum \ below \ enum \ e
           Opens key:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             1.0.7.3_\5&34baf594&0&0.0.0
           Opens key:
                                                                                                                                                                  HKLM \setminus system \setminus current control set \setminus enum \setminus pciide \setminus idechannel \setminus 4\&20064 fa2\&0\&1
```

```
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34\
   Opens key:
   Opens key:
                                           HKLM\system\wpa\478c035f-04bc-48c7-b324-2462d786dad7-5p-9\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10\
  Opens kev:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12\
  Opens kev:
                                           HKLM\svstem\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15\
   Opens key:
                                           Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19\
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\
   Opens key:
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25\
   Opens key:
                                           \label{localization} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\label{localization}
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31\
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32\
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33\
  Opens key:
   Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4\
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5\
  Opens kev:
                                           HKLM\svstem\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6\
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7\
  Opens key:
  Opens key:
                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8\
  Opens key:
                                           Opens key:
                                           HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{88d96a06 - f192 - 11d4 - a65f - f192 - f1
0040963251e5}
                                           HKCR\activatableclasses\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
   Opens key:
   Opens key:
                                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
                                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\treatas
  Opens key:
   Opens key:
                                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32
                                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:
   Opens kev:
                                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:
                                           HKLM\software\microsoft\msxm160
                                           Opens key:
0040963251e53
   Opens key:
                                           HKCR \land activatable classes \land clsid \land \{88d96a08-f192-11d4-a65f-0040963251e5\}
   Opens key:
                                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
   Opens key:
                                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\treatas
   Opens key:
                                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\ \ \ in procserver 32
   Opens key:
                                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler32
   Opens key:
                                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:
                                           HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}
                                           HKCR\activatableclasses\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
   Opens key:
   Opens kev:
                                           HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
  Opens key:
                                           HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
                                           HKCR \verb|\clsid| \{0f87369f-a4e5-4cfc-bd3e-73e6154572dd\} \verb|\inprocserver32|
  Opens key:
  Opens key:
                                           Opens key:
                                           HKCR \clsid \end{area} a 4e5-4cfc-bd3e-73e6154572dd \end{area} in prochandler and the second secon
   Opens key:
                                           HKLM\system\currentcontrolset\control\productoptions
   Opens key:
                                           HKLM\system\currentcontrolset\services\wpdbusenum
   Opens key:
                                           HKLM\system\currentcontrolset\services\wpdbusenum\parameters
  Opens key:
                                           {\it HKLM} \verb|\software\microsoft\windows\currentversion\action
center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:
                                           HKLM\software\microsoft\windowsruntime\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}
  Opens kev:
                                           HKCR\activatableclasses\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens kev:
                                           HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:
                                           HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:
                                           HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\treatas
   Opens key:
                                           HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
   Opens key
                                           HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32
   Opens key:
                                           HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
   Opens key:
                                           HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprochandler32
                                           HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
   Opens kev:
   Opens key:
                                           HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprochandler
                                           HKCR\clsid\{9} dac2c1e-7c5c-40eb-833b-323e85a1ce84\}\ \ in prochandler
   Opens key:
  Opens key
                                           HKLM\software\microsoft\security center
   Opens key
                                           HKLM\software\policies\microsoft\internet explorer\security
  Opens key:
                                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens key:
                                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
```

```
settings\zones\1
                                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
 settings\zones\2
    Opens key:
                                                                  \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3
                                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zones\4
                                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\zones\0
    Opens key:
                                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
    Opens key:
                                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
    Opens key:
                                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zones\3
    Opens kev:
                                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
    Opens key:
                                                                  HKCU\software\policies\microsoft\internet explorer
                                                                  HKCU\software\microsoft\internet explorer\security
    Opens key:
                                                                  HKLM\software\microsoft\internet explorer\security
    Opens kev:
    Opens key:
                                                                  HKCU\software\microsoft\windows\currentyersion\internet settings\zones
    Opens key:
                                                                  HKLM\software\microsoft\windows\currentversion\internet settings\zones
    Opens key:
                                                                  HKLM\system\currentcontrolset\services\wscsvc\startoverride
    Opens key:
                                                                  HKLM\software\policies\microsoft\windows defender
    Opens key:
                                                                  HKLM\software\policies\microsoft\windows defender\real-time protection
    Opens key:
                                                                  HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}
    Opens key:
                                                                  HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{ca236752 - 2e77 - 4386 - b63b - b6
0e34774a413d}
    Opens key:
                                                                  HKCR\activatableclasses\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
    Opens key:
                                                                  HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
                                                                  HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\treatas
                                                                  HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
    Opens kev:
    Opens key
                                                                  HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32
    Opens key:
                                                                  HKCR \ clsid \ \{ca236752-2e77-4386-b63b-0e34774a413d\} \ inprocserver 32
                                                                  HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
    Opens key:
0e34774a413d}\inprochandler32
    Opens key:
                                                                 HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
    Opens key:
                                                                  HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler
                                                                  HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
    Opens kev:
                                                                  HKLM\software\policies\microsoft\windows\windows error reporting
    Opens key:
    Opens kev:
                                                                  HKCU\software\policies\microsoft\windows\windows error reporting
                                                                  HKCU\software\microsoft\windows\windows error reporting
    Opens key:
    Opens key:
                                                                  HKLM\software\microsoft\windows\windows error reporting\syspreplock
    Opens key:
                                                                  HKCU\software\microsoft\windows\windows error reporting\erc
    Opens key:
                                                                  HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 's ession in fo' 1
    Opens key:
Opens key:
                                                                  HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{88d96a05 - f192 - 11d4 - a65f - f192 - f1
0040963251e5}
    Opens key:
                                                                  HKCR\activatableclasses\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
                                                                  HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
    Opens key:
    Opens kev:
                                                                  HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
                                                                  HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
    Opens key:
0040963251e5}\treatas
                                                                  HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
    Opens key:
    Opens key:
                                                                  HKCU \setminus software \setminus classes \setminus clsid \setminus \{88d96a05 - f192 - 11d4 - a65f - f192 - f
0040963251e5}\inprocserver32
     Opens key:
                                                                  HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
    Opens key:
                                                                  HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprochandler32
                                                                 HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\ \ in prochandler 32
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprochandler
                                                                 HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
    Opens kev:
    Opens key:
                                                                  HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
    Opens kev:
                                                                  HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3be-belle + belle + belle
499afcec98c4}
    Opens key:
                                                                  HKCR\activatableclasses\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
    Opens key:
                                                                  HKCU \setminus software \setminus classes \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3be - 499afcec98c4\}
    Opens key:
                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
                                                                  HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
    Opens key:
499afcec98c4}\treatas
    Opens key:
                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
                                                                 HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
    Opens key:
499afcec98c4}\inprocserver32
                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
    Opens key:
    Opens key:
                                                                  HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprochandler32
                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
    Opens key:
    Opens key
                                                                  HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprochandler
    Opens key:
                                                                 HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\
     Opens key:
                                                                  HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
```

Opens key: f0aa6db5d4bc} Opens key: HKCR\activatableclasses\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc} HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc} Opens key: Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc} HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-Opens kev: f0aa6db5d4bc}\treatas Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas Opens key f0aa6db5d4bc}\inprocserver32 Opens key:  $HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32$ Opens key HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2f0aa6db5d4bc}\inprochandler32 Opens key:  $HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler32$ HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-Opens key f0aa6db5d4bc}\inprochandler Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler Opens key: HKLM\software\microsoft\windows\currentversion\explorer HKLM\software\microsoft\windows\currentversion\action Opens key: center\providers\com\{d26de5c1-c061-43f7-9c40-7517526cf1c1} HKLM\software\microsoft\windowsruntime\clsid\{d26de5c1-c061-43f7-9c40-Opens key: 7517526cf1c1} Opens key: HKCR\activatableclasses\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1} Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{d26de5c1-c061-43f7-9c40-7517526cf1c1\}$ Opens key:  $HKCR\clsid\d26de5c1-c061-43f7-9c40-7517526cf1c1$ Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas Opens key: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32 HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32 Opens kev: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-Opens key: 7517526cf1c1}\inprochandler32 HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler32 Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-Opens kev: 7517526cf1c1}\inprochandler Opens key:  $HKCR\clsid\d26de5c1-c061-43f7-9c40-7517526cf1c1\$ \inprochandler Opens key HKCU\software\microsoft\windows\currentversion\startupnotify HKLM\software\microsoft\windows\currentversion\action Opens key: center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{6ae07dc1-0244-4c6f-9ab0-144$ 5017a56357c3} Opens key: HKCR\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} Opens kev: HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} Opens key: HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-Opens key 5017a56357c3} HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} Opens kev: Opens key  $HKCU \setminus software \setminus classes \setminus activatable classes \setminus clsid \setminus \{6ae07dc1-0244-4c6f-9ab0-1$ 5017a56357c3}  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ action$ Opens key:  $center \verb|\providers| eventlog \verb|\final {01979c6a-42fa-414c-b8aa-eee2c8202018} |$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowswindowsbackup/actioncenter Opens kev: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswindowsbackup/actioncenter HKLM\software\microsoft\windowsruntime\clsid\{900c0763-5cad-4a34-bc1f-Opens key: 40cd513679d53 HKCR\activatableclasses\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5} Opens key Opens key HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5} Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5} Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-Opens key: 40cd513679d5}\inprocserver32 Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32 HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-Opens key 40cd513679d5}\inprochandler32 HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32 Opens key: Opens key HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler Opens kev:  $HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\$  inprochandler HKLM\software\microsoft\windows\currentversion\action Opens key  $center \verb|\providers| eventlog \verb|\dab69a6a-4d2a-4d44-94bf-e0091898c881| \}$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsnetworkaccessprotection/whc Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/who HKLM\software\microsoft\windows\currentversion\action Opens kev: center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78} HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-Opens key: windows defender/whc Opens key:  $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -windows \ -windows$ defender/whc HKLM\software\microsoft\windows\currentversion\action

center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}

Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsdiagnosis-scheduled/operational Opens key:  $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -diagnosis-diagnosi$ scheduled/operational HKLM\software\microsoft\windows\currentversion\action Opens kev: center\providers\eventlog\{de7b24ea-73c8-4a09-985d-5bdadcfa9017} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowstaskscheduler/maintenance Opens key:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ taskscheduler/maintenance  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ action$  $center \verb|\providers| eventlog \verb|\final 134ea 407-755d-4a 93-b8a6-f290cd 155023 \}$  $\label{lem:hklm} \verb+Kklm \system \current control set \services \$ Opens key: homegroup control panel/operational Opens key: control panel/operational HKLM\software\microsoft\windows\currentversion\action Opens kev: center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowssecurity-spp-ux-notifications/actioncenter Opens key:  $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -security \ -spp-ux-like \ -windows \ -security \ -windows \ -security \ -spp-ux-like \ -windows \ -security \ -spp-ux-like \ -windows \ -security \ -windows \ -security \ -spp-ux-like \ -windows \ -security \ -spp-ux-like \ -windows \ -security \ -windows \ -security \ -windows \ -security \ -windows \ -security \ -windows \ -wind$ notifications/actioncenter Opens key: HKLM\software\microsoft\windows\currentversion\action  $center \verb|\providers| eventlog \verb|\space| b447b4db-7780-11e0-ada3-18a90531a85a \}$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsfilehistory-core/whc Opens kev: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistorycore/whc  ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action}$ Opens key:  $center \verb|\providers| eventlog \verb|\f37a1c-a68d-4d6e-8c9b-f79e8b16c482|$ Opens key:  $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ event \+ log \+ microsoft - windows - log \+ microsoft - w$ ntfs/whc Opens key:  $HKLM \ software \ microsoft\ windows \ - trentversion \ winevt\ channels\ microsoft\ - windows\ - tfs/whc$ Opens kev: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5} HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-shell-Opens key: connectedaccountstate/actioncenter Opens kev: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter  ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action}$ Opens key:  $center \providers \eventlog \end{496f4a050-7e31-453c-88be-9634f4e02139}$ Opens key:  $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ event \+ log \+ microsoft - windows - log \+ microsoft - w$ userpnp/actioncenter Opens key:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/actioncenter Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsstoragespaces-managementagent/whc Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc Opens key: HKLM\software\microsoft\windows\currentversion\action center Opens key:  $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{96f4a050-7e31-453c-88be-164a050-7e31-4500-7e31$ 9634f4e02139} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsuserpnp/scheduleroperations Opens key:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ userpnp/scheduleroperations HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-Opens key: userpnp/performance Opens key  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/performance  $\label{lem:hklm} \verb+Kklm \system \current control set \services \$ Opens key: userpnp/devicemetadata/debug Opens key:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/devicemetadata/debug Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries value: HKCU\control panel\desktop[preferreduilanguages] HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Oueries value: Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus side by side [prefer external manifest]$ Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]

nt\currentversion\compatibility32[conhost]

HKLM\software\microsoft\windows

```
Oueries value:
                                     HKLM\system\currentcontrolset\control\cmf\config[system]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\windows[loadappinit_dlls]
                                     HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:
  Queries value:
                                     HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                                     HKLM\software\microsoft\ole[aggressivemtatesting]
  Oueries value:
  Oueries value:
                                     HKCU\console[screencolors]
                                     HKCU\console[popupcolors]
  Oueries value:
                                     HKCU\console[insertmode]
  Oueries value:
  Oueries value:
                                     HKCU\console[quickedit]
  Oueries value:
                                     HKCU\console[codepage]
  Oueries value:
                                     HKCU\console[screenbuffersize]
  Queries value:
                                     HKCU\console[windowsize]
  Queries value:
                                     HKCU\console[windowposition]
                                     HKCU\console[fontsize]
  Queries value:
                                     HKCU\console[fontfamily]
  Oueries value:
  Queries value:
                                     HKCU\console[fontweight]
  Queries value:
                                     HKCU\console[facename]
  Queries value:
                                     HKCU\console[cursorsize]
  Oueries value:
                                     HKCU\console[historvbuffersize]
  Oueries value:
                                     HKCU\console[numberofhistorybuffers]
  Oueries value:
                                     HKCU\console[historynodup]
  Oueries value:
                                     HKCU\console[colortable00]
  Queries value:
                                     HKCU\console[colortable01]
  Oueries value:
                                     HKCU\console[colortable02]
                                     HKCU\console[colortable03]
  Queries value:
  Queries value:
                                     HKCU\console[colortable04]
  Queries value:
                                     HKCU\console[colortable05]
  Oueries value:
                                     HKCU\console[colortable06]
  Queries value:
                                     HKCU\console[colortable07]
                                     HKCU\console[colortable08]
  Oueries value:
  Queries value:
                                     HKCU\console[colortable09]
  Oueries value:
                                     HKCU\console[colortable101
  Oueries value:
                                     HKCU\console[colortable111
  Oueries value:
                                     HKCU\console[colortable121
  Queries value:
                                     HKCU\console[colortable13]
  Oueries value:
                                     HKCU\console[colortable14]
  Queries value:
                                     HKCU\console[colortable15]
  Queries value:
                                     HKCU\console[loadconime]
  Oueries value:
                                     HKCU\console[extendededitkey]
  Queries value:
                                     HKCU\console[extendededitkeycustom]
  Queries value:
                                     HKCU\console[worddelimiters]
  Queries value:
                                     HKCU\console[trimleadingzeros]
  Oueries value:
                                     HKCU\console[enablecolorselection]
  Oueries value:
                                     HKCU\console[scrollscale]
  Oueries value:
                                     HKLM\software\microsoft\samclient\windows[ceipenable]
                                     Oueries value:
  Oueries 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]
                                     HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                     HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicv[enabled]
                                     HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Oueries value:
  Oueries value:
                                     {\tt HKLM \setminus software \setminus microsoft \setminus ctf[enable anchor context]}
  Oueries value:
HKLM \verb|\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]
                                     HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
  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 \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]] \ details a side by side \ details a side \ details a side by side \ details a side
  Oueries value:
                                     HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Oueries 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]
  Oueries value:
                                     HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
                                     HKLM\system\setup[oobeinprogress]
  Oueries value:
                                     HKLM\svstem\setup[svstemsetupinprogress]
  Oueries value:
                                     HKLM\software\microsoft\rpc[idletimerwindow]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Oueries value:
                                     HKLM\software\microsoft\com3[com+enabled]
                                     HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
  Oueries value:
  Queries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32 [alg]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
  Queries value:
                                     HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
```

HKLM\software\microsoft\ole[defaultaccesspermission]

Queries value:

```
Queries value:
                                   HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
                                   Queries value:
cryptographic provider[type]
                                   Queries value:
cryptographic provider[image path]
                                   HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Oueries value:
  Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds]
  Oueries value:
                                   HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Oueries value:
                                   HKLM\software\microsoft\cryptography[machineguid]
                                   Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                   HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_misc]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_cm]
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_svc]
                                   \label{local-operator} \mbox{HKLM} \mbox{$\sf Software} \mbox{$\sf microsoft} \mbox{$\sf msdtc} \mbox{$\sf tracing} \mbox{$\sf sources} \mbox{$\sf [trace\_gateway]$}
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_ui]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_contact]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
  Oueries value:
                                   \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \software \microsoft \mbox{$\mbox{$m$sdtc$tracing$} sources[trace\_cluster]$} \end{tabular}
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_resource]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_tip]
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
  Queries value:
  Queries value:
                                   HKLM \setminus software \setminus microsoft \setminus msdtc \setminus tracing \setminus sources[trace\_log]
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_ktmrm]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_vssbackup]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_tm]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_wmi]
  Oueries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ msdtc\+ tracing\+ output\+ [tracefile path]
  Queries value:
                                   HKLM\software\microsoft\msdtc\tracing\output[memorybuffersize]
                                   {\tt HKLM \coftware \microsoft \msdtc \tracing \coutput[debugoutenabled]}
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\misc[disabletracing]
                                   HKLM\software\microsoft\msdtc[noparallellogflushnotification]
  Oueries value:
  Queries value:
HKLM\software\microsoft\msdtc[snapshotprefertransactionstimeoutduringbackup]
                                   HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[disableterminationonheapcorruption]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc[sysprepinprogress]
                                   HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
  Oueries value:
  Oueries value:
                                   HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\description[]
  Oueries 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[]
                                   HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol[]
  Oueries value:
  Queries value:
                                   HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint[]
                                   HKCR\cid.local\15546232-d044-45d4-88a8-
  Queries value:
Ob84583f2fe1\customproperties\log\size[1
                                   HKLM\software\microsoft\msdtc\mtxoci[oraclexalibpath]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc\mtxoci[oraclesgllibpath]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\mtxoci[oracleocilibpath]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
  Queries value:
                                   HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
  Queries value:
                                   HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
                                   HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
  Queries value:
  Queries value:
                                   HKLM\software\microsoft\msdtc\security[accountname]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\security[networkdtcaccess]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
  Queries value:
                                   HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
  Queries value:
                                   HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\security[xatransactions]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\security[lutransactions]
                                   HKCR\cid.local\15546232-d044-45d4-88a8-
  Queries value:
Ob84583f2fe1\customproperties\log\path[]
  Queries value:
                                   HKLM \ system \ current control \ wmi \ security [1b1d4ff4-f27b-4c99-f27b] \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the control \ wmi \ security \ defined a simple of the \ defined 
8bd7-da8f1a74051a]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
  Queries value:
                                   HKLM\software\microsoft\windows
\verb|nt\currentversion| tracing \verb|msdtc| logging options[maxbuffers]|
                                   HKLM\software\microsoft\windows
  Oueries value:
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 \verb|\system| current control \verb|\timezone information[standard name]|
```

```
Oueries value:
                                           HKLM\system\currentcontrolset\control\timezoneinformation[standardbias]
                                           HKLM\system\currentcontrolset\control\timezoneinformation[standardstart]
   Queries value:
                                           HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
   Queries value:
                                           HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
   Queries value:
   Queries value:
                                           HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]
                                           HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\tracing\msdtc\modules[uniqueid]
                                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\tracing\msdtc\modules[active]
  Oueries 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]
                                           HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
                                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
  Oueries value:
                                           HKLM\software\microsoft\windows
\verb| nt\currentversion \rangle is decimal to the control of the control 
                                           HKLM\system\currentcontrolset\control\wmi\security[e80aa9fe-913d-4ede-
  Oueries value:
af58-73e332dcac8d1
   Queries value:
                                           HKLM\software\microsoft\msdtc[dtcmaxsessions]
   Oueries 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]
   Oueries value:
                                           HKLM\software\microsoft\msdtc[waitforallxabranchprepares]
   Queries value:
                                           HKLM\software\microsoft\msdtc\security[snapshotsecuritydisabled]
                                           HKLM\software\microsoft\msdtc[servertcpport]
   Oueries value:
                                           HKLM\software\microsoft\windows nt\currentversion[currentversion]
   Queries value:
   Oueries value:
                                           HKLM\software\microsoft\msdtc[cmcancelrpcafter]
   Oueries value:
                                           HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
                                           HKLM\software\microsoft\msdtc[cmmaxidlepings]
   Oueries value:
   Queries value:
                                           HKLM\software\microsoft\msdtc[cmpingfreqsecs]
   Oueries value:
                                           HKLM\software\microsoft\msdtc[cmverbose]
   Queries value:
                                           HKLM\software\microsoft\msdtc[rpcqoscapabilities]
                                           HKLM\software\microsoft\msdtc[rpcqosidentity]
   Queries value:
   Oueries 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[]
                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host[]
   Oueries value:
                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid[]
   Oueries value:
                                           HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
   Oueries value:
                                           \label{local-4452c425-ad2f-4cde-b895-734b166ac4ac} HKCR \cid.local \allocal \allocal \allocal \cid.local \allocal \cid.local \allocal \cid.local \allocal \cid.local \allocal \cid.local \allocal \cid.local \cid.local \allocal \cid.local \cid
   Oueries value:
                                           HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint[]
   Oueries value:
   Oueries value:
                                           HKCU\control panel\international[scurrencyoverride]
   Oueries 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]
                                           HKLM\software\microsoft\rpc\securityservice[9]
   Queries value:
   Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
   Queries value:
   Oueries value:
                                           HKLM \setminus system \setminus current control \setminus lsa \setminus spicache \setminus credssp.dll[comment]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
   Queries value:
   Queries value:
                                           Queries value:
                                           HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
   Oueries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus credssp.dll[tokensize]
                                           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:
   Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                           HKLM\software\microsoft\msdtc[shared memory mutex timeout]
   Queries value:
                                           HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host[]
   Oueries value:
   Oueries value:
                                           HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid[]
   Oueries value:
                                           HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
   Oueries value:
                                           HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol[]
   Queries value:
                                           HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\endpoint[]
   Queries value:
                                           HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
                                           HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
   Queries value:
                                           HKLM\software\microsoft\msdtc[transactionbridge]
   Oueries value:
   Queries value:
                                           HKLM\software\microsoft\msdtc[logwarnenabled]
   Queries value:
                                           HKLM\software\microsoft\msdtc[suppressduplicateduration]
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
   Queries value:
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-
   Oueries value:
b913c40c9cd4}\inprocserver32[inprocserver32]
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
   Oueries value:
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-
   Oueries value:
b913c40c9cd4}\inprocserver32[threadingmodel]
   Queries value:
                                           HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
   Oueries value:
                                           HKLM\software\microsoft\msdtc[supportns]
   Queries value:
                                           HKLM\system\currentcontrolset\services\keyiso[objectname]
   Queries value:
                                           HKLM\system\currentcontrolset\services\eaphost[imagepath]
```

Oueries value: HKLM\system\currentcontrolset\services\eaphost[wow64]

HKLM\system\currentcontrolset\services\eaphost[objectname] Queries value:

HKLM\system\currentcontrolset\services\eaphost[requiredprivileges] Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\reliability[timestampinterval] HKLM\hardware\description\system\centralprocessor\0[~mhz] Oueries value:

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ appxdeploymentserver/operational[type]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ appxdeploymentserver/operational[enabled]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ appxdeploymentserver/operational[filemax]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ appxdeploymentserver/operational[filecounter]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[buffersize]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ appxdeploymentserver/operational[minbuffers]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ appxdeploymentserver/operational[maxbuffers]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ appxdeploymentserver/operational[latency]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[clocktype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[sidtype]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ appxdeploymentserver/operational[level]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[controlguid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[maxsize]

Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ appxdeploymentserver/operational[maxsizeupper] Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ appxdeploymentserver/operational[retention]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ appxdeploymentserver/operational[autobackuplogfiles]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[file]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsappxdeploymentserver/operational[filterid]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ appxdeploymentserver/operational[isolation]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ appxdeploymentserver/operational[owningpublisher]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ appxdeploymentserver/operational[channelaccess]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ networkprofile/operational[type]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ networkprofile/operational[enabled]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ networkprofile/operational[filemax]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ networkprofile/operational[filecounter]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkprofile/operational[buffersize]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkprofile/operational[minbuffers]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot winevt \cdot channels \setminus microsoft - windows - windows$ networkprofile/operational[maxbuffers]

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkprofile/operational[latency]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkprofile/operational[clocktype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkprofile/operational[sidtype]

Queries value:

 $\label{thm:loss-twindows-universion-winevt-channels-microsoft-windows-network-profile/operational[level] \\$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} wincrosoft-windows-network profile/operational [control guid]$ 

Oueries value

 $HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} Which is the label{lem:hklm} Which is the label{lem:hkklm} Which i$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[maxsizeupper]

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows - network profile/operational \cite{loss} \cite{loss$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} hkll \label{lem:hklm} Winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hkklm} hkll \label{lkklm} hkll \la$ 

Queries value:

 $HKLM \label{local-bound} HKLM \label{local-bound} Software \label{local-bound} Windows \label{local-bound} Like \label{local-bound} HKLM \label{local-bound} Software \label{local-bound} Windows \label{local-bound} If it expressed as a function of the property of the p$ 

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} etwork profile/operational [filterid]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lklm} \label{lem:hklm} \label{lklm} \$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkprofile/operational[channelaccess]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-kernel-storem \scalebox{\color=line-windows-kernel-storem} winevt\channels \microsoft-windows-kernel-storem \scalebox{\color=line-windows-kernel-storem \scalebox{\color=line-windows-kernel-storem} winevt\channels \microsoft-windows-kernel-storem \scalebox{\color=line-windows-kernel-storem} winevt\channel\scalebox{\color=line-windows-kernel-storem \scalebox{\color=line-windows-kernel-s$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows-kernel-storem \scale="like-storemgr/operational" [enabled] \\$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernelstoremgr/operational[filemax]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-kernel-storem \scalebox{\$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-kernel-storemgr/operational[buffersize]$ 

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-kernel-storem \scalebox{\colorable}{lem:loss} winevt \channels \microsoft-windows-kernel-storem \scalebox{\colorable}{lem:loss} winevt \microsoft-windows-kernel-storem \scalebox{\colora$ 

Queries value:

 $\label{thm:local_max} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-kernel-storem \gray \$ 

Oueries value:

 $\label{thm:hammels} HKLM\software\microsoft-windows-kernel-storemgr/operational [latency]$ 

Queries value:

Queries value.

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernelstoremgr/operational[clocktype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernelstoremgr/operational[sidtype]

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-kernel-storem \gray \gray$ 

Queries value:

 $\label{thm:local-problem} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-kernel-storem \graph{\mathbb{graph}}\ \columnwise \channels \microsoft \-windows \-kernel-storem \graph\graph \graph \g$ 

Queries value:

 $\label{thm:local_maxsize} HKLM \software \microsoft-windows-kernel-storem \scalebox{\scalebox[windows]{\sc$ 

Queries value:

 $\label{thm:local_max} HKLM \software \microsoft-windows-kernel-storem \scalebox{\colorable} rotation al \microsoft-windows-kernel-storem \scalebox{\colorable} rotation \scalebox{\color$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft \windows \- kernel-storem \ gr/operation al \ [retention]$ 

Oueries value:

 $\label{thm:local} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-kernel-storem \end{substant} roperation al \cite{thm:local} autoback \cite{thm:local} roperation \cite{thm:local}$ 

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - kernel-part \ windows \ - kernel-part \ - kernel-part$ storemgr/operational[file]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernelstoremgr/operational[filterid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-kernelstoremgr/operational[isolation]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - kernel-like \ microsoft \ windows - kernel-like \ windows$ storemgr/operational[owningpublisher]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - kernel-like \ windows \ - kernel-like \ windows \ - kernel-like \ - ke$ storemgr/operational[channelaccess]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ devicesetupmanager/operational[type]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the property of the prope$ devicesetupmanager/operational[enabled]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ devicesetupmanager/operational[filemax]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ devicesetupmanager/operational[filecounter]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ devicesetupmanager/operational[buffersize]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[minbuffers]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[maxbuffers]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ devicesetupmanager/operational[latency]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[clocktype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[sidtype]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ devicesetupmanager/operational[level] Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ devicesetupmanager/operational[controlguid]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ devicesetupmanager/operational[maxsize]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[maxsizeupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[retention]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ devicesetupmanager/operational[autobackuplogfiles]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ devicesetupmanager/operational[file]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ devicesetupmanager/operational[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsdevicesetupmanager/operational[isolation]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ devicesetupmanager/operational[owningpublisher]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ devicesetupmanager/operational[channelaccess]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ userpnp/deviceinstall[type]

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} windows \end{tabular} consoft \end{tabular} windows \end{tabular} and \end{tabular} windows \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} windows \end{tabular} w$ userpnp/deviceinstall[enabled]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[filemax]

Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the substitution of the subs$ userpnp/deviceinstall[filecounter]

```
Oueries value:
```

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[buffersize]

Oueries value

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hkklm} Win$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[maxbuffers]

Oueries value:

 $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} Winevt \label{limits} Wine$ 

Queries value:

 $HKLM \label{lem:hklm} In the constant of the$ 

Queries value

 $\label{thm:loss-twindows-user-problem} HKLM \software \end{area} Windows \soft-windows \soft-windo$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[level]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} winevt \label{lem:hklm} Variety \label{lem:hklm} winevt \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Windows \label{lem:hklm} Variety \label{lem:hklm} Variet$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lklm} winevt \label{lklm} winevt \label{lklm} winevt \label{lklm} winevt \label{lklm} winevt$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[maxsizeupper]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[retention]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/deviceinstall[filterid]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Queries value:

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

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[wow64]

Queries value: HKLM\system\currentcontrolset\services\ui0detect[requiredprivileges]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

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] Oueries value: 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)] HKLM\software\microsoft\windows\currentversion[programw6432dir] Oueries value: Oueries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir1 Oueries value:  $\label{lem:hard-windows} HKLM \software \mbox{$\mbox{$\mbox{$m$icrosoft}\windows}$ nt \current version \profile list \scales -1-5-profile \scales -1-5-$ 

18[profileimagepath]

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[appdata]

 $Queries\ value: \\ HKU\.default\software\microsoft\windows\currentversion\explorer\usershell\ folders[local\ appdata]$ 

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]
Oueries 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]

```
Oueries value:
                                                                                                                                                  HKLM\system\currentcontrolset\services\sharedaccess[dependonservice]
                                                                                                                                                  HKLM\system\currentcontrolset\services\sharedaccess[dependongroup]
           Queries value:
                                                                                                                                                  HKLM\system\currentcontrolset\services\sharedaccess[group]
           Queries value:
           Queries value:
                                                                                                                                                  HKLM\system\currentcontrolset\services\sharedaccess[objectname]
          Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{54849625-5478-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4994-a5ba-4964-a5ba-4964-a5ba-4994-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-496-a5b
```

3e3b0328c30d}[]

Oueries value:

3e3b0328c30d}[messagefilename]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{54849625-5478-4994-a5ba-4964-a5ba-4964-a5ba-4994-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-496-a5b$ 3e3b0328c30d}[categorymessagefile]

Queries value:

3e3b0328c30d}[resourcefilename]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{54849625-5478-4994-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-496-a5b$ 3e3b0328c30d}[parameterfilename]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{54849625-5478-4994-a5ba-4964-a5ba-4964-a5ba-4994-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-4964-a5ba-496-a5b$ 3e3b0328c30d}[helplink]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{54849625-5478-4994-a5ba-494-a5ba-494-a5ba-494-a5ba-494-a5ba-494-a5ba-494-a5ba-494-a5ba-494-a5$ 3e3b0328c30d}[enabled]

 $HKLM \setminus software \\ \mbox{$154849625-5478-4994-a5ba-bc.} \label{eq:hklm} HKLM \setminus software \\ \mbox{$154849625-5478-4994-a5ba-bc.} \label{eq:hklm} HKLM \setminus software \\ \mbox{$154849625-5478-4994-a5ba-bc.} \label{eq:hklm}$ 3e3b0328c30d}[categorycount]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{555908d1-a6d7-4695-8e1e-16464, and a software \ microsoft \ windows \ not the software \ microsoft \ mi$ 26931d2012f4}[1

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus publishers \setminus \{555908d1 - a6d7 - 4695 - 8e1e - a6d7 -$ 26931d2012f4}[messagefilename]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[categorymessagefile]

Queries value:

26931d2012f4}[resourcefilename]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-4600-8e1e-4695-8e1e-4695-8e$ 26931d2012f4}[parameterfilename]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[helplink]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[enabled]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-a6d7-4605-8e1e-a605-8e1e-a6$ 26931d2012f4}[categorycount]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}\channelreferences[count1

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-4600-8e1e-4695-8e1e-4695-8e$ 26931d2012f4}\channelreferences\0[] Oueries value:

26931d2012f4}\channelreferences\0[flags]

Queries value:

26931d2012f4}\channelreferences\0[id]

Queries value: HKLM\system\currentcontrolset\services\eventlog\system\service control manager[providerguid]

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] HKLM\system\currentcontrolset\services\pnrpsvc[tag] Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\pnrpsvc[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\pnrpsvc[dependongroup] Oueries 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] Oueries 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] HKLM\system\currentcontrolset\services\appidsvc[wow64] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\appinfo[imagepath] Oueries value: HKLM\system\currentcontrolset\services\appinfo[wow64] Oueries value: HKLM\system\currentcontrolset\services\appmgmt[imagepath] Oueries value: HKLM\system\currentcontrolset\services\appmgmt[wow64] Queries value: HKLM\system\currentcontrolset\services\axinstsv[imagepath] Oueries value: HKLM\system\currentcontrolset\services\axinstsv[wow64] Queries value: HKLM\system\currentcontrolset\services\bdesvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\bdesvc[wow64]

Oueries value: HKLM\system\currentcontrolset\services\bits[imagepath] HKLM\system\currentcontrolset\services\bits[wow64] Queries value: HKLM\system\currentcontrolset\services\bthserv[imagepath] Queries value: HKLM\system\currentcontrolset\services\bthserv[wow64] Queries value: Queries value: HKLM\system\currentcontrolset\services\cscservice[imagepath] HKLM\system\currentcontrolset\services\cscservice[wow64] Oueries value: Oueries value:

HKLM\system\currentcontrolset\services\deviceassociationservice[imagepath]

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\deviceassociationservice[wow64] Oueries value:

HKLM\system\currentcontrolset\services\dnscache[imagepath] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache[wow64] Oueries value: HKLM\system\currentcontrolset\services\dot3svc[imagepath] Queries value: HKLM\system\currentcontrolset\services\dot3svc[wow64] Oueries value: HKLM\system\currentcontrolset\services\dsmsvc[imagepath] HKLM\system\currentcontrolset\services\dsmsvc[wow64] Queries value: HKLM\system\currentcontrolset\services\efs[imagepath] Oueries value: Queries value: HKLM\system\currentcontrolset\services\efs[wow64] Oueries value: HKLM\system\currentcontrolset\services\fdphost[imagepath] HKLM\system\currentcontrolset\services\fdphost[wow64] Queries value: HKLM\system\currentcontrolset\services\fdrespub[imagepath] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\fdrespub[wow64] Oueries value: HKLM\system\currentcontrolset\services\fhsvc[imagepath] Oueries value:  $HKLM \verb|\system| current control set \verb|\services| fhsvc[wow64]|$ Queries value: HKLM\system\currentcontrolset\services\hidserv[imagepath] Oueries value: HKLM\system\currentcontrolset\services\hidserv[wow64] HKLM\system\currentcontrolset\services\hkmsvc[imagepath]

Queries value: HKLM\system\currentcontrolset\services\hkmsvc[wow64] Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[imagepath] HKLM\system\currentcontrolset\services\homegrouplistener[wow64] Oueries value: Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[imagepath] Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[wow64]

Queries value: HKLM\system\currentcontrolset\services\ktmrm[imagepath] Oueries value: HKLM\system\currentcontrolset\services\ktmrm[wow64] Oueries value: HKLM\system\currentcontrolset\services\lltdsvc[imagepath] HKLM\system\currentcontrolset\services\lltdsvc[wow64] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\mpssvc[imagepath] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus mpssvc[wow64]$ Queries value: HKLM\system\currentcontrolset\services\msiscsi[imagepath] HKLM\system\currentcontrolset\services\msiscsi[wow64] Queries value: Oueries value: HKLM\system\currentcontrolset\services\napagent[imagepath] Queries value: HKLM\system\currentcontrolset\services\napagent[wow64] Oueries value: HKLM\system\currentcontrolset\services\ncasvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\ncasvc[wow64] Oueries value: HKLM\system\currentcontrolset\services\ncdautosetup[imagepath]

Oueries value: HKLM\system\currentcontrolset\services\ncdautosetup[wow64] Oueries value: HKLM\system\currentcontrolset\services\netlogon[imagepath]  $HKLM \verb|\system| current controlset \verb|\services| netlogon[wow64]|$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\netman[imagepath] Oueries value: HKLM\system\currentcontrolset\services\netman[wow64]

Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\peerdistsvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[wow64] Queries value: HKLM\system\currentcontrolset\services\pla[imagepath] Oueries value: HKLM\system\currentcontrolset\services\pla[wow64]

Oueries value: HKLM\system\currentcontrolset\services\pnrpautoreg[imagepath] Oueries value: HKLM\system\currentcontrolset\services\pnrpautoreg[wow64] Oueries value: HKLM\system\currentcontrolset\services\pnrpsvc[wow64] Oueries value:  ${\tt HKLM} \verb| system| current control set| services| print notify[image path]$ Queries value: HKLM\system\currentcontrolset\services\printnotify[wow64] Oueries value: HKLM\system\currentcontrolset\services\qwave[imagepath] Queries value: HKLM\system\currentcontrolset\services\qwave[wow64] HKLM\system\currentcontrolset\services\rasauto[imagepath] Queries value: Queries value: HKLM\system\currentcontrolset\services\rasauto[wow64] Oueries value: HKLM\system\currentcontrolset\services\rasman[imagepath] Oueries value: HKLM\system\currentcontrolset\services\rasman[wow64]

Queries value: HKLM\system\currentcontrolset\services\remoteaccess[imagepath] Queries value: HKLM\system\currentcontrolset\services\remoteaccess[wow64] Oueries value: HKLM\system\currentcontrolset\services\remoteregistry[imagepath] Oueries value: HKLM\system\currentcontrolset\services\remoteregistry[wow64] Oueries value: HKLM\system\currentcontrolset\services\scardsvr[imagepath] Oueries value: HKLM\system\currentcontrolset\services\scardsvr[wow64] Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[wow64] HKLM\system\currentcontrolset\services\seclogon[imagepath] Queries value: Oueries value: HKLM\system\currentcontrolset\services\seclogon[wow64] Queries value: HKLM\system\currentcontrolset\services\sensrsvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\sensrsvc[wow64] HKLM\system\currentcontrolset\services\sharedaccess[wow64] Queries value: HKLM\system\currentcontrolset\services\sstpsvc[imagepath] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\sstpsvc[wow64] Oueries value: HKLM\svstem\currentcontrolset\services\storsvc[imagepath] HKLM\system\currentcontrolset\services\storsvc[wow64] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\svsvc[imagepath]

Oueries value: HKLM\system\currentcontrolset\services\tabletinputservice[imagepath] Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[wow64]

HKLM\system\currentcontrolset\services\svsvc[wow64]

Queries value: HKLM\system\currentcontrolset\services\tapisrv[imagepath]

```
HKLM\system\currentcontrolset\services\threadorder[imagepath]
  Queries value:
                          HKLM\system\currentcontrolset\services\threadorder[wow64]
  Queries value:
  Queries value:
                          HKLM\system\currentcontrolset\services\upnphost[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\upnphost[wow64]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\vaultsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vaultsvc[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vmicheartbeat[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vmicheartbeat[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vmickvpexchange[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vmickvpexchange[wow64]
 Oueries 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 \setminus system \setminus current control set \setminus services \setminus vmicshutdown[wow64]
  Oueries value:
                          HKLM\system\currentcontrolset\services\vmictimesync[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\vmictimesync[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vmicvss[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\vmicvss[wow64]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\w32time[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\w32time[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wbiosrvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wbiosrvc[wow64]
 Queries value:
                          HKLM\system\currentcontrolset\services\wcncsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wcncsvc[wow64]
                          HKLM\system\currentcontrolset\services\wcspluginservice[imagepath]
  Queries value:
 Queries value:
                          Queries value:
                          HKLM\system\currentcontrolset\services\wdisystemhost[imagepath]
  Oueries value:
                          HKLM\system\currentcontrolset\services\wdisystemhost[wow64]
 Queries value:
                          HKLM\system\currentcontrolset\services\webclient[imagepath]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\webclient[wow64]
 Queries value:
                          HKLM\system\currentcontrolset\services\wecsvc[imagepath]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\wecsvc[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wercplsupport[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wercplsupport[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wersvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wersvc[wow64]
 Queries value:
                          HKLM\system\currentcontrolset\services\wiarpc[imagepath]
  Queries value:
                          HKLM\system\currentcontrolset\services\wiarpc[wow64]
  Oueries value:
                          HKLM\system\currentcontrolset\services\winrm[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\winrm[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wlansvc[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\wlansvc[wow64]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\wlidsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wlidsvc[wow641
 Oueries value:
                          HKLM\system\currentcontrolset\services\wpcsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wpcsvc[wow64]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wscsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\wscsvc[wow64]
 Oueries 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]
  Oueries value:
                          HKLM\system\currentcontrolset\services\wwansvc[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\wwansvc[wow64]
                          HKLM\system\currentcontrolset\services\p2pimsvc[requiredprivileges]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\p2psvc[requiredprivileges]
                          HKLM \verb|\system| current controlset \verb|\services| pnr pautoreg[required privileges]|
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\pnrpsvc[requiredprivileges]
                          \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\profilelist\s-1-5-} \\
 Queries value:
19[profileimagepath]
 Queries value:
                          HKU \ s-1-5-19 \ software \ microsoft \ windows \ current version \ explorer \ user
shell folders[appdata]
                          HKU\s-1-5-19\software\microsoft\windows\currentversion\explorer\user
  Queries value:
shell folders[local appdata]
  Queries value:
                          HKLM\system\currentcontrolset\services\p2pimsvc[environment]
  Oueries value:
                          HKLM\system\currentcontrolset\services\p2pimsvc[startprotected]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\svchost[localservicepeernet]
 Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile[sychost]
 Oueries value:
                          HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
 Oueries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemanifest]
                          HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain]
 Queries value:
  Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
                          HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
 Oueries value:
 Queries value:
                          HKLM\software\policies\microsoft\peernet[disabled]
 Queries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedllunloadonstop]
 Oueries value:
                          HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll1]
 Oueries value:
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]
 Queries value:
                          HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
 Oueries value:
                          HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
```

HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout]

HKLM\system\currentcontrolset\services\tapisrv[wow64]

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num]
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[next\_catalog\_entry\_id]
   Oueries value:
- Queries value:

  HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9\inum catalog entries641
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries64]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000001[packedcatalogitem]

  Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\0000000000004[packedcatalogitem]
   Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries 64 \ 00000000000006 \ [packed catalog item] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000008[packedcatalogitem]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\000000000009[packedcatalogitem]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries64]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000001[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000001[displaystring]
- $\label{local-bound} HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries 64 \000000000001 \cite{MKLM} \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\00000000001[addressfamily]
   Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries 64 \000000000001 \[supported namespace]\queries value:$
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries 64 \000000000001 \cite{lemabled} \end{substitute} Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\00000000001[providerinfo] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries 64 \0000000000002 [library path] \\ Queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000002[displaystring]
   Oueries value:

- $\label{lem:hklm} HKL $$M \simeq \end{subarray} In $M \simeq \end{su$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\0000000000002[storesserviceclassinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries 64 \ 0000000000002 [provider in fo] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000003[providerid] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries 64 \0000000000003 \[address family]\ Queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000003[supportednamespace]

  Queries value:

  HKLM\system\surrentsentrolset\services\winsock2\parameters\namespace\_catalog\_entries64\000000000003[supportednamespace]
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog5 \catalog\_entries 64 \000000000003 \catalog\_entries 64 \catalog \services \catalog \system \system \catalog \system$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\00000000003[version] Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries 64 \ 0000000000003 \ [storesservice class in fo] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000004[librarypath]
  Oueries 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[addressfamily]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000004[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000004[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000004[storesserviceclassinfo] Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries 64 \ 0000000000004 \ [providerinfo] \ Queries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000005[librarypath]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000005[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000005[providerid]
 Oueries 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\00000000005[enabled]
 Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries 64 \000000000005 \[version] \names \nam$ 

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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000006[librarypath]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000006[displaystring] Queries value:

 $\label{lem:hklm/system/current} HKLM\system\current\controlset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\0000000000006[providerid]\ Queries\value:$ 

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries 64 \0000000000006 \[address family] \queries value:$ 

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries 64 \0000000000006 \[supported namespace]\quaries 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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\000000000006[providerinfo]
Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 numhandle buckets]$ 

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32spincount]

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Oueries value:

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

in6[winsock 2.0 provider id]

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [used elayed acceptance]$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-

806e6f6e6963}[enabledhcp]

Queries value:

55779daa70e9}[registrationenabled]

Queries value:

55779daa70e9}[registeradaptername]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus interfaces \setminus \{b5105d63-74c6-4dc1-87b7-14c6-4dc1-87b7-80b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-4dc1-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-14c6-87b7-8$ 

55779daa70e9}[domain]

Oueries 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:

806e6f6e6963}[registeradaptername]

Queries value:

```
806e6f6e6963}[domain]
   Queries value:
806e6f6e6963}[dhcpdomain]
                                          HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
                                          HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\compatibilitv32[svchost1
                                          HKLM\software\microsoft\samclient[machineid]
   Oueries value:
                                          \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \label{lklmsoftware} \begi
   Oueries value:
linklocal\linklocal_ff00::%12/8[seedserver]
   Queries value:
                                          \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows nt\- current version\+ pernet\+ pnrp\+ ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastpublish]
   Queries value:
                                          \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\sc pernet\pnrp\ipv6-} \\
linklocal\linklocal_ff00::%12/8[disablemulticastsearch]
   Queries value:
                                          \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows nt\- current version\+ pernet\+ 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]
                                          HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
  Queries value:
linklocal\linklocal_ff00::%12/8[mincpalifetime]
                                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[appdata]
   Oueries value:
                                          HKLM \verb|\system| current controlset \verb|\services| crypt 32 [debugheapflags]|
   Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
                                          HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
   Queries value:
   Queries value:
                                          HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
   Queries value:
                                          HKLM \ software \ microsoft \ rsa
schannel cryptographic provider[type]
  Queries value:
                                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
schannel cryptographic provider[image path]
                                          HKLM\software\policies\microsoft\cryptography[forcekeyprotection]
   Queries value:
                                          HKLM\system\currentcontrolset\services\plugplay[imagepath]
   Oueries value:
                                          HKLM\system\currentcontrolset\services\plugplay[type]
   Oueries value:
                                          HKLM\system\currentcontrolset\services\plugplay[start]
   Oueries value:
   Queries value:
                                          HKLM\system\currentcontrolset\services\plugplay[errorcontrol]
   Oueries value:
                                          HKLM\system\currentcontrolset\services\plugplay[tag]
   Queries value:
                                          HKLM\system\currentcontrolset\services\plugplay[dependonservice]
                                          HKLM\system\currentcontrolset\services\plugplay[dependongroup]
   Queries value:
   Oueries 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:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]
  Oueries value:
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
   Oueries value:
                                          {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
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]

 ${\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\$ Queries value:

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]

Oueries value:

HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedllunloadonstop] Oueries value: HKLM\svstem\currentcontrolset\services\spooler[imagepath] HKLM\system\currentcontrolset\services\spooler[type] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\spooler[start] Oueries value: HKLM\system\currentcontrolset\services\spooler[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\spooler[tag] Queries value: HKLM\system\currentcontrolset\services\spooler[dependonservice]

Oueries value: HKLM\system\currentcontrolset\services\spooler[dependongroup] Queries value: HKLM\system\currentcontrolset\services\spooler[group] HKLM\system\currentcontrolset\services\spooler[objectname] Queries value: Queries value: HKLM\system\currentcontrolset\services\http[objectname] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\spooler[requiredprivileges]

Oueries value: HKLM\system\currentcontrolset\services\spooler[environment] Oueries value:  $\label{lem:hklm} \verb+Kklm \software \microsoft \windows nt \current version \mbox{\verb+limage file execution}$ 

options\spoolsv.exe[usefilter]

Queries value:  $\label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution$ options\spoolsv.exe[debugger]

Queries value:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\spoolsv.exe[uselargepages]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[nodeoptions]

HKLM\software\microsoft\windows nt\currentversion\image file execution Queries value: options\spoolsv.exe[disablewakecharge]

Oueries 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:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ 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]
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value:
options\spoolsv.exe[tracingflags]
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[minimumstackcommitinbytes]
                                   \begin{tabular}{ll} HKLM\software\mbox{\begin{tabular}{ll} \line & \
  Oueries value:
options\spoolsv.exe[breakoninitializeprocessfailure]
  Queries value:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[keepactivationcontextsalive]
  Queries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\spoolsv.exe[trackactivationcontextreleases]
  Queries value:
                                   \label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\sc mage file execution} \\
options\spoolsv.exe[maxdeadactivationcontexts]
  Queries value:
                                   \label{lem:hklm} \verb+Kklm \software \microsoft \windows nt \current version \mbox{\verb+limage file execution}
options\spoolsv.exe[globalflag]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[cwdillegalindllsearch]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value:
options\spoolsv.exe[debugprocessheaponly]
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value:
options\spoolsv.exe[searchpathmode]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\compatibility32[spoolsv]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\rpcss[imagepath]
                                   HKLM\system\currentcontrolset\services\rpcss[type]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\rpcss[start]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rpcss[errorcontrol]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\rpcss[tag]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rpcss[dependonservice]
                                   HKLM\system\currentcontrolset\services\rpcss[dependongroup]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\rpcss[group]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\wmi\security[d2e1bab2-eb9b-4ba7-
9123-19c01ddc4f781
                                   HKLM\system\currentcontrolset\control\wmi\security[c9bf4a9e-d547-4d11-
  Oueries value:
8242-e03a18b5be011
  Oueries value:
                                   \label{lem:hamler} \verb|HKLM\| system \| current control \| control \| print[exception handler enabled]|
  Queries value:
                                   ae24-ebc9b8676e76]
  Oueries 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]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\print[maxrpccalls]
                                   HKLM\software\microsoft\sqmclient\windows\disabledprocesses[71e8376c]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\sqmclient\windows[studyid]
                                   HKLM \verb|\software\m| icrosoft \verb|\telemetryclient\samplestore\sqm[sampledout]|
  Oueries value:
  Oueries value:
                                   HKLM \verb|\system| current controlset| control \verb|\print[callexitprocess on shutdown]|
  Oueries value:
                                   HKLM\system\currentcontrolset\services\seclogon[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\seclogon[start]
  Queries value:
                                   HKLM\system\currentcontrolset\services\seclogon[errorcontrol]
                                   HKLM\system\currentcontrolset\services\seclogon[tag]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\seclogon[dependonservice]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\seclogon[dependongroup]
  Queries value:
                                   HKLM\system\currentcontrolset\services\seclogon[group]
  Queries value:
                                   HKLM\system\currentcontrolset\services\seclogon[objectname]
                                   HKLM\system\currentcontrolset\services\seclogon[requiredprivileges]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sens[imagepath]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sens[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\sens[start]
  Oueries value:
                                   {\tt HKLM \setminus system \setminus current controlset \setminus services \setminus sens[error control]}
  Queries value:
                                   HKLM\system\currentcontrolset\services\sens[tag]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sens[dependonservice]
  Queries value:
                                   HKLM\system\currentcontrolset\services\sens[dependongroup]
                                   HKLM\system\currentcontrolset\services\sens[group]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\sens[objectname]
  Oueries 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]
                                   HKLM\system\currentcontrolset\services\sysmain[type]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sysmain[start]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sysmain[errorcontrol]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sysmain[tag]
  Queries value:
                                   HKLM\system\currentcontrolset\services\sysmain[dependonservice]
  Queries value:
                                   HKLM\system\currentcontrolset\services\sysmain[dependongroup]
                                   HKLM\system\currentcontrolset\services\sysmain[group]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\sysmain[objectname]
  Queries value:
                                   HKLM\system\currentcontrolset\services\schedule[imagepath]
  Queries value:
                                   HKLM\system\currentcontrolset\services\schedule[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\schedule[start]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\schedule[errorcontrol]
                                   HKLM\svstem\currentcontrolset\services\schedule[tag]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\schedule[dependonservice]
                                   HKLM\system\currentcontrolset\services\schedule[dependongroup]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\schedule[group]
  Queries value:
                                   HKLM\system\currentcontrolset\services\schedule[objectname]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\lmhosts[imagepath]
  Queries value:
                                   HKLM\system\currentcontrolset\services\lmhosts[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\lmhosts[start]
```

```
Oueries value:
                          HKLM\system\currentcontrolset\services\lmhosts[errorcontrol]
                          HKLM\system\currentcontrolset\services\lmhosts[tag]
  Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts[dependonservice]
  Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts[group]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\lmhosts[objectname]
 Oueries value:
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
 Queries value:
                          HKLM\system\currentcontrolset\services\afd[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\tcpip[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\tdx[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\netbt[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts[wow64]
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts[requiredprivileges]
                          HKLM\system\currentcontrolset\services\vss[imagepath]
  Queries value:
  Oueries 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]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vss[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vss[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\vss[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\vss[objectname]
  Queries value:
HKLM\system\currentcontrolset\services\lmhosts\parameters[enableusermode]
                          HKLM\system\currentcontrolset\services\vss[wow64]
  Queries value:
  Queries value:
                          HKLM\system\currentcontrolset\services\vss[environment]
  Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[e14dcdd9-d1ec-4dc3-
8395-a606df8ef1151
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[4d20df22-e177-4514-
a369-f1759feedeb3]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
 Oueries value:
                          HKLM\software\microsoft\com3\finalizeractivitybvpass1
                          HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
 Oueries value:
                          HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}[]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\vss\settings[idletimeout]
 Oueries value:
                          HKLM\system\setup[upgradeinprogress]
 Oueries value:
HKLM\system\currentcontrolset\services\vss\settings[activewriterstatetimeout]
  Oueries 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]
                          HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocserver32[threadingmodel]
                          HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[1
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Oueries 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]
                          HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[threadingmodel]
 Oueries value:
                          HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[start]
 Oueries value:
                          \label{lem:hklm} \verb+Kklm \+ system \+ current control \+ wmi \+ autologger \+ circular \+ kernel
context logger[flushthreshold]
 Queries value:
                          \label{lem:hklm} \verb+Kklm \+ system \+ current 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]
 Oueries value:
                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filename]
                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
 Oueries value:
context logger[enablekernelflags]
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[stackwalkingfilter]
                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
 Queries value:
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]
                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
 Queries value:
context logger[disablerealtimepersistence]
                          HKCR\interface\\\ 609b954b-4fb6-11d1-9971-00c04fbbb345\\\\proxystubclsid32[]
 Oueries value:
                          {\tt HKLM \ } system \verb|\ current control \verb|\ wmi \ | autologger \verb|\ circular| kernel \\
 Oueries value:
context logger[guid]
 Oueries value:
                          \label{lem:hklm} \verb+Kklm \system \current control \window mi \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]
                                                                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
      Queries value:
context logger[stackcaching]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-
af71-3e63d056f174]
                                                                                   HKCR\interface\{00000100-0000-0000-0000-00000000046}\proxystubclsid32[]
     Oueries value:
                                                                                   HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
     Oueries value:
                                                                                   HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
     Oueries value:
                                                                                   HKCR\clsid\{7542e960-79c7-11d1-88f9-
     Oueries value:
0080c7d771bf}\inprocserver32[inprocserver32]
                                                                                   HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
      Queries value:
     Queries value:
                                                                                   HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocserver32[threadingmodel]
      Queries value:
                                                                                   HKCR \ interface \ \{609b9557-4fb6-11d1-9971-00c04fbbb345\} \ proxystubclsid32[]
      Queries value:
HKLM\system\currentcontrolset\services\audiosrv\parameters[servicedllunloadonstop]
     Queries value:
                                                                                   HKLM\software\microsoft\windows
nt\currentversion\windows[displayversion]
                                                                                   HKCU\control panel\desktop[paintdesktopversion]
     Queries value:
     Oueries value:
HKLM\system\currentcontrolset\services\eventlog\application\vss[providerguid]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[imagepath]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[type]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[start]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[errorcontrol]
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[tag]
     Queries value:
     Queries value:
                                                                                   {\tt HKLM \ } system \verb| current control set \verb| services \verb| audiosrv[dependon service] 
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[dependongroup]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[group]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[objectname]
     Oueries value:
                                                                                   HKLM\svstem\currentcontrolset\services\mmcss[objectname]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\audioendpointbuilder[objectname]
     Oueries value:
                                                                                   HKLM\svstem\currentcontrolset\services\audiosrv[wow64]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\audiosrv[requiredprivileges]
     Oueries value:
                                                                                   HKLM\svstem\currentcontrolset\services\wersvc[type]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\wersvc[start]
     Oueries value:
                                                                                   {\tt HKLM \ } system \verb| current control set \verb| services \verb| wersvc[error control]|
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\wersvc[tag]
      Queries value:
                                                                                   HKLM\system\currentcontrolset\services\wersvc[dependonservice]
      Oueries 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]
                                                                                   HKLM\system\currentcontrolset\services\sysmain[wow64]
     Oueries value:
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\wersvc[requiredprivileges]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\wersvc[environment]
     Oueries value:
                                                                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ svchost\+ [wersvcgroup]
     Queries value:
                                                                                   HKU\.default\control panel\international[scurrencyoverride]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\wersvc\parameters[servicedll]
     Queries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicemanifest]
                                                                                   {\tt HKLM \controlset \control
      Queries value:
                                                                                   HKLM\system\currentcontrolset\control\wmi\security[6851adeb-79da-4250-
      Oueries value:
a440-f1f52d28711d]
     Queries value:
                                                                                   HKLM\software\microsoft\windows\windows error reporting[servicetimeout]
     Oueries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicedllunloadonstop]
     Oueries value:
                                                                                   HKLM\svstem\currentcontrolset\services\mpssvc[tvpe]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\mpssvc[start]
     Oueries value:
                                                                                   {\tt HKLM \ } system \verb| current control set \verb| services \verb| mpssvc[error control]|
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\mpssvc[tag]
     Oueries value:
                                                                                   HKLM\system\currentcontrolset\services\mpssvc[dependonservice]
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\mpssvc[dependongroup]
                                                                                   HKLM\system\currentcontrolset\services\mpssvc[group]
      Queries value:
     Queries value:
                                                                                   HKLM\system\currentcontrolset\services\mpssvc[objectname]
     Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{6bba3851-2c7e-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f
31e5afd029e3}[1
     Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-
31e5afd029e3}[messagefilename]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{6bba3851-2c7e-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f
31e5afd029e3}[categorymessagefile]
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{6bba3851-2c7e-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54
31e5afd029e3}[resourcefilename]
     Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-
31e5afd029e3}[parameterfilename]
     Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{6bba3851-2c7e-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f
31e5afd029e3}[helplink]
     Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-
31e5afd029e3}[enabled]
     Oueries value:
HKLM \ software \ icrosoft \ windows \ current version \ winevt \ publishers \ \ \{6bba3851-2c7e-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f54-4dea-8f5
31e5afd029e3}[categorycount]
```

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnosis \-debug[type]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/debug[enabled]

Queries value:

 $\label{lem:hklmsoft} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/debug[filemax]$ 

Oueries value:

 $HKLM \label{linear_li$ 

Oueries value

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/debug[buffersize]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/debug[minbuffers]

Queries value:

 $\label{thm:local-microsoft-windows-diagnosis-debug[maxbuffers]} HKLM \software \mbox{\winevt\channels\mbox{\winevt\channels\mbox{\winevt\channels\mbox{\winevt\channels\channels\winevt\channels\mbox{\winevt\channels\channels\winevt\channels\winevt\channels\channels\winevt\channels\winevt\channels\winevt\channels\winevt\channels\channels\winevt\cha$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - diagnosis-dps/debug[latency]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/debug[clocktype]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - diagnosis-dps/debug[sidtype]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-diagnosis-dps/debug[level]$ 

Queries value:

 $\label{thm:local-microsoft-windows-diagnosis-debug[keywords]} HKLM \software \mbox{\winevt\channels\mbox{\winevt\channels\mbox{\winevt\channels\mbox{\winevt\channels\winevt\channels\winevt\channels\mbox{\winevt\channels\$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} cosoft-windows - diagnosis-dps/debug[keywordsupper]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/debug[controlguid]

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} cosoft-windows - diagnosis-dps/debug[maxsize]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/debug[maxsizeupper]$ 

Queries value: KLM\software

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - diagnosis-dps/debug[retention]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - diagnosis-dps/debug[autobackuplogfiles]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \wincosoft \windows \current version \winevt \channels \wincosoft \windows \-diagnosis-dps/debug[file]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} Current \label{lem:hklm} Windows \label{lem:hklm} Current \label{lem:hklm} Windows \label{lem:hkklm} Windows \label{lem:hkk$ 

Queries value:

 $\label{thm:hammelsmicrosoft-windows-diagnosis-described} HKLM\software\microsoft-windows-diagnosis-dps/debug[isolation]$ 

Queries value:

 $\label{thm:local-prop} HKLM \noothware \nicrosoft-windows \noothware \nooth$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/debug[channelaccess]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/operational[type]

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/operational[enabled]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/operational[filemax]$ 

Queries value:

 $\label{thm:local_hammels_microsoft-windows-diagnosis-dps/operational[filecounter]} HKLM\software\mbox{\constraints} winevt\channels\mbox{\constraints} microsoft-windows-diagnosis-dps/operational[filecounter]$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows-diagnosis-dps/operational [buffersize]$ 

Queries value:

 $\label{thm:local_microsoft} HKLM \software \microsoft-windows-diagnosis-dps/operational[minbuffers]$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/operational[maxbuffers]$ 

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/operational[latency]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/operational[clocktype]

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/operational[sidtype]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/operational[level]$ 

Oueries value

 $\label{thm:local} HKLM \software \microsoft-windows-diagnosis-dps/operational [control guid]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/operational[maxsize]

Queries value:

 $\label{thm:local_hammels} HKLM \software \wincosoft-windows-diagnosis-dps/operational[maxsizeupper]$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/operational \cite{thm:local-windows-diagnosis-dps/operational}.$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows-diagnosis-dps/operational [autobackuplogfiles]$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/operational [file]$ 

Queries value: KLM\software

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} Consider \label{lem:hklm} Windows \label{lem:hklm} Consider \label{lem:hklm} Windows \label{lem:hkklm} Windows \label{lem:hkklm$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-diagnosis-dps/operational[isolation]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \-diagnosis-dps/operational[owningpublisher]$ 

Queries value:

 $\label{thm:local_HKLM} HKLM \label{thm:local_HKLM} HKLM \label{thm:local_HKLM} HKLM \label{thm:local_HKLM} irrosoft-windows-diagnosis-dps/operational[channelaccess]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/analytic[type]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnosis-dps/analytic[enabled]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \wincosoft \windows \current version \winevt \channels \wicrosoft \-windows \-diagnosis \-dps/analytic \[filemax]$ 

Queries value:

 $HKLM \label{linear_li$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/analytic[buffersize]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-diagnosis-dps/analytic \microsoft-windows-dps/analytic \microsoft-win$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/analytic \cite{label{local-prop}} maxbuffers \cite{label{local-prop}} \end{subarrange}$ 

Queries value:

 $\label{thm:local-prop} HKL\begin{tabular}{l} HKL\begin{tabular}{$ 

Queries value:

Queries value:

HKLMNsoftware\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdos/analytic[clocktype]

Queries value:

RKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic[sidtype]

Queries value:

RELEGIBLE STATES S

Queries value:

 $\label{thm:local-prop} HKLM \software \wicrosoft \windows \current version \winevt \channels \wicrosoft \-windows \-diagnosis-dps/analytic \cite{thm:local-prop} \end{supplies} Analytic \cite{thm:local-pro$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \wincosoft \windows \current version \winevt \channels \wincosoft \windows \-diagnosis-dps/analytic \cite{thm:local-prop} and \cite{th$ 

Oueries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/analytic[controlguid]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - diagnosis-dps/analytic[maxsize]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows - diagnosis-dps/analytic[maxsizeupper]$ 

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic[retention]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic[autobackuplogfiles]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic[file]

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/analytic [filterid]$ 

Oueries value

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnosis-dps/analytic [isolation]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic[owningpublisher]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic[channelaccess]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{cfc18ec0-96b1-4eba-961b-622caee05b0a\}[]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{cfc18ec0-96b1-4eba-961b-622caee05b0a\} \ [messagefilename]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorymessagefile]

Oueries value:

 $\label{like:hklm} HKLM \software \mbox{$microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[resourcefilename]$$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{cfc18ec0-96b1-4eba-961b-622caee05b0a\} \ [parameter filename]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\currentversion} \winevt\publishers \cfc18ec0-96b1-4eba-961b-622caee05b0a} \ [helplink]$ 

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\mbox{$\mbox{}\mbox{$\mbox$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{cfc18ec0-96b1-4eba-961b-622caee05b0a\} \ [category count]$ 

Queries value:

Queries value:

 $\label{thm:local_microsoft} HKLM \software \microsoft-windows-diagnostics-performance/operational[enabled]$ 

Queries value

 $\label{lem:hklm} HKLM \software \microsoft-windows-diagnostics-performance/operational[filemax]$ 

Queries value:

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-diagnostics-performance/operational[buffersize]$ 

Oueries value:

Queries value

Queries value:

 $\label{thm:local_hammels} HKLM \label{thm:local_hammels} If the local like the$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-diagnostics-performance/operational[clocktype]$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostic s-performance \software \climate{local} \climate{l$ 

Queries value

 $\label{lem:hklm} HKLM \software \sincos of twindows - diagnostic speciform ance/operational [level]$ 

Queries value:

 $\label{thm:local} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostics-performance/operational \cite{thm:local-performance}. The local \cite{thm:local-performance} \$ 

Queries value:

 $\label{thm:local_maxsize} HKLM \software \microsoft-windows-diagnostics-performance/operational[maxsize]$ 

Queries value:

 $\label{thm:local_maxsize} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostics-performance \software \microsoft \-windows \-diagnostics-performance \-di$ 

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows \- current version \winevt \channels \microsoft-windows - diagnostic specific mance/operational \cite{thm:loss} and \cite{thm:loss} a$ 

performance/operational[autobackuplogfiles]

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/operational[file]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/operational[filterid]

Oueries value:

performance/operational[isolation]

performance/operational[owningpublisher]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic services - diagnosti - diagnostic services - diagnostic services - diagnostic service$ performance/operational[channelaccess]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[type]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[enabled]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic services - diagnosti - diagnostic services - diagnostic services - diagnostic service$ performance/diagnostic[filemax]

Queries value:

performance/diagnostic[filecounter]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[buffersize]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostic s \ -diagno$ performance/diagnostic[minbuffers]

Queries value:

performance/diagnostic[maxbuffers]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[latency]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[clocktype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[sidtype] Queries value:

performance/diagnostic[level]

performance/diagnostic[keywordslower] Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[keywordsupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[controlguid]

Oueries value:

performance/diagnostic[maxsize]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostic s \ -diagno$ performance/diagnostic[maxsizeupper]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic services - diagnosti - diagnostic services - diagnostic services - diagnostic service$ performance/diagnostic[retention]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[autobackuplogfiles]

Queries value:

performance/diagnostic[file]

performance/diagnostic[filterid]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostic s \ -diagno$ performance/diagnostic[isolation]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[owningpublisher]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-diag$ performance/diagnostic[channelaccess]

Oueries value:

performance/diagnostic/loopback[type]

performance/diagnostic/loopback[enabled]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic services - diagnosti - diagnostic services - diagnostic services - diagnostic service$ performance/diagnostic/loopback[filemax]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostic s \ -diagno$ performance/diagnostic/loopback[filecounter]

Oueries value:

performance/diagnostic/loopback[buffersize]

performance/diagnostic/loopback[minbuffers]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic services - diagnosti - diagnostic services - diagnostic services - diagnostic service$ performance/diagnostic/loopback[maxbuffers]

Queries value:

performance/diagnostic/loopback[latency]

Queries value:

performance/diagnostic/loopback[clocktype]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic services - diagnosti - diagnostic services - diagnostic services - diagnostic service$ performance/diagnostic/loopback[sidtype]

Queries value:

performance/diagnostic/loopback[level]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[keywordslower]

Oueries value:

performance/diagnostic/loopback[keywordsupper]

Queries value:

performance/diagnostic/loopback[controlguid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[maxsize]

Queries value:

performance/diagnostic/loopback[maxsizeupper]

Oueries value:

performance/diagnostic/loopback[retention]

Queries value:

performance/diagnostic/loopback[autobackuplogfiles]

performance/diagnostic/loopback[file]

Oueries value:

 $HKLM \label{lem:hkk} In the constant of the$ performance/diagnostic/loopback[filterid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[isolation]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[owningpublisher]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostics \ -diagnos$ performance/diagnostic/loopback[channelaccess]

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] Oueries value: HKLM\system\currentcontrolset\services\stisvc[tag]

Oueries value: HKLM\system\currentcontrolset\services\stisvc[dependonservice] Queries value: HKLM\system\currentcontrolset\services\stisvc[dependongroup] Oueries 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] Oueries 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]

Oueries value:

HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest]

HKLM\system\currentcontrolset\services\stisvc\parameters[servicemain] Oueries value: Queries value:

 $HKLM \setminus system \setminus current control \setminus stillimage \setminus trace[suppressproces soutput]$ 

Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[maxfilesize]

Oueries value:

HKLM\system\currentcontrolset\control\stillimage\trace[defaulttraceflags]

Queries value:  $HKLM \setminus system \setminus current control \setminus stillimage \setminus trace[default trace mask]$ 

Oueries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracelevel] HKLM\system\currentcontrolset\control\stillimage\trace[defaultmaxtracearraysize] Queries value: HKLM\svstem\currentcontrolset\control\stillimage\trace[defaultenableobiecttracking] Oueries value: HKLM\system\currentcontrolset\control\stillimage\trace[heapoptions] Oueries value:  $HKLM \setminus system \setminus current control \setminus stillimage \setminus trace \setminus wiaservc. dll[traceflags]$ Oueries value: Queries value: Queries value:  $HKLM \setminus system \setminus current control \setminus stillimage \setminus trace \setminus wiaservc.dll[maxtracearraysize]$ Oueries value: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[enableobjecttracking] Queries value: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[heapoptions] Oueries value: HKLM\software\microsoft\rpc\securityservice[10] Oueries value:  $HKCR \cdot Appid \cdot \{a1f4e726-8cf1-11d1-bf92-0060081ed811\} [authenticationlevel]$  $HKCR \land appid \land \{a1f4e726-8cf1-11d1-bf92-0060081ed811\} [access permission]$ Queries value: Oueries value: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: HKLM\software\microsoft\windows\currentversion[devicepath] HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}[] Queries value: Queries value: HKLM\system\currentcontrolset\control\stillimage[deviceid] Queries value: Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected[guid] Oueries value: HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[name] Oueries value:  $HKLM \ system \ current control \ stillimage \ events \ connected \ \{ee1ddf29-1c65-4ea6-b5cc-1c65-4ea6-b5c-1c65-4ea6-b5$ 6c15f82b5905}[desc] Oueries value:  $HKLM \ system \ current control \ stillimage \ events \ connected \ \{ee1ddf29-1c65-4ea6-b5cc-1c64-4ea6-b5c-1c64-4ea6-b5c-$ 6c15f82b5905}[icon] Oueries value: HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[cmdline] Queries value: HKLM\system\currentcontrolset\control\stillimage\events\disconnected[defaulthandler] Oueries 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] Oueries value: 759eb35cdf9a}[name] Queries value: 759eb35cdf9a}[desc] Queries value: HKLM\system\currentcontrol\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon] Oueries value 759eb35cdf9a}[cmdline] Queries value:  $HKLM \ system \ `current control \ stillimage \ `events \ faximage [defaulth and ler]$ HKLM\system\currentcontrolset\control\stillimage\events\faximage[guid] Queries value: Queries value: 759eb35cdf9a}[name] Oueries value: 759eb35cdf9a}[desc] Oueries value: HKLM\system\currentcontrol\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon] Oueries 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\currentcontrol\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name1 Oueries value: HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc] Oueries value: 759eb35cdf9a}[icon] 

```
759eb35cdf9a}[cmdline]
      Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[defaulthandler]
      Queries value:
                                                                              Queries value:
783ce7a92f22}[name1
    Oueries value:
783ce7a92f22}[desc1
     Oueries value:
HKLM \ system \ current control \ stillimage \ events \ scan but ton \ \{5f4baad0-4d59-4fcd-b213-b213-b214, \ b213-b214, 
783ce7a92f22}[icon]
    Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}[cmdline1
     Queries value:
759eb35cdf9a}[name]
     Oueries value:
759eb35cdf9a}[desc]
    Oueries value:
759eb35cdf9a}[icon]
     Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[cmdline]
     Oueries value:
HKLM \ system \ current control \ stillimage \ events \ scanbutton \ \{eabbd70d-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96a-a25f-4e90-96
7105fd3b53b1}[name]
    Queries value:
7105fd3b53b1}[desc]
    Oueries value:
7105fd3b53b1}[icon]
     Queries value:
7105fd3b53b1}[cmdline]
    Queries value:
HKLM \ system \ control \ stillimage \ events \ scan button \ \{ee1ddf29-1c65-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5c-4ea6-b5c-4ea6-b5c-
6c15f82b5905}[name]
    Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-
6c15f82b5905}[desc]
     Queries value:
HKLM \ system \ current control \ stillimage \ events \ scan but ton \ \{ee1ddf29-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5cc-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6-b5c-1c65-4ea6
6c15f82b5905}[icon]
     Oueries value:
HKLM \ system \ control \ stillimage \ events \ scan button \ \{ee1ddf29-1c65-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5cc-4ea6-b5c-4ea6-b5c-4ea6-b5c-4ea6-b5c-4ea6-b5c-4ea6-b5c-4ea6-b5c-4ea6
6c15f82b5905}[cmdline]
     Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[defaulthandler]
     Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[guid]
    Oueries value:
HKLM\system\currentcontrolset\control\stillimage\serversettings[shutdownifunuseddelay]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[type]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[start]
     Oueries value:
                                                                              {\tt HKLM \ } system \verb| current control set \verb| services \verb| w32time[error control]|
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[tag]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[dependonservice]
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[dependongroup]
                                                                              HKLM\system\currentcontrolset\services\w32time[group]
     Queries value:
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[objectname]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\w32time[requiredprivileges]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[type]
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[start]
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[tag]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[dependonservice]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[dependongroup]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[group]
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\dnscache[objectname]
     Queries value:
                                                                              HKLM\system\currentcontrolset\services\wuauserv[imagepath]
                                                                              HKLM\system\currentcontrolset\services\wuauserv[type]
     Queries value:
     Oueries 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]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\wuauserv[dependongroup]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\wuauserv[group]
     Oueries value:
                                                                              HKLM\system\currentcontrolset\services\wuauserv[objectname]
```

HKLM\system\currentcontrolset\services\wlansvc[tag] Queries value: HKLM\system\currentcontrolset\services\wlansvc[dependonservice] Queries value: HKLM\system\currentcontrolset\services\wlansvc[dependongroup]

Oueries value: Oueries value:

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\wlansvc[type]

HKLM\system\currentcontrolset\services\wlansvc[start]

HKLM\system\currentcontrolset\services\wlansvc[errorcontrol]

```
Oueries value:
                                                    HKLM\system\currentcontrolset\services\wlansvc[group]
                                                    HKLM\system\currentcontrolset\services\wlansvc[objectname]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\wcmsvc[objectname]
    Queries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\ndisuio[objectname]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\nativewifip[objectname]
                                                    HKLM\system\currentcontrolset\services\nativewifip[imagepath]
    Oueries value:
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\nativewifip[type]
                                                    HKLM\svstem\currentcontrolset\services\nativewifip[pnpflags]
    Oueries value:
                                                    HKLM\system\currentcontrolset\control\wmi\security[d905ac1c-65e7-4242-
   Queries value:
99ea-fe66a8355df81
    Queries value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
    Queries value:
                                                    HKLM \ system \ current control \ network \ \{4d36e974-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filtertype]
                                                    HKLM \ system \ current control \ network \ \{4d36e974-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterruntype]
                                                   HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Queries value:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterclass]
                                                   HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Queries value:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindonattach]
                                                   HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Oueries value:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindondetach]
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\ndisuio[imagepath]
    Queries value:
HKLM \setminus system \setminus current control set \\ + num \setminus pci \setminus ven\_8086\& dev\_100e\& subsys\_001e8086\& rev\_02 \setminus 3\&267a616a\&1\&18[driver]
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Queries value:
08002be10318}\0010\linkage[upperbind]
    Queries value:
                                                    HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\ndisuio[type]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\ndisuio[pnpflags]
                                                    HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-
   Oueries value:
aded-5304bf8f636d]
    Oueries value:
                                                    HKLM\system\currentcontrolset\control\wmi\securitv\b3eee223-d0a9-40cd-
adfc-50f1888138ab1
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\ndisuio[legacypause]
    Queries value:
                                                    HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
    Oueries value:
                                                    08002be10318}\0007\linkage[upperbind]
                                                    HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
    Queries value:
    Oueries value:
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage[upperbind]
    Queries value:
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage[upperbind]
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\ndisuio[ndisbootstart]
                                                    HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
    Oueries value:
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value:
08002be10318\} \verb|\| 0004 \verb|\| linkage[upperbind]|
    Oueries value:
                                                    HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[driver]
    Oueries value:
                                                    08002be10318}\0000\linkage[upperbind]
                                                    HKLM\system\currentcontrolset\services\wlansvc[requiredprivileges]
    Queries value:
    Oueries value:
55779daa70e9}[searchlist]
                                                    HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
    Oueries value:
    Queries value:
                                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage[upperbind]
                                                    HKLM\system\currentcontrolset\enum\root\*isatap\0000[driver]
    Oueries value:
    Oueries value:
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage[upperbind]
    Oueries value:
                                                    HKLM\system\currentcontrolset\enum\root\*teredo\0000[driver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0012\linkage[upperbind]
    Queries value:
                                                    HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
    Oueries value:
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage[upperbind]
    Queries value:
                                                    HKLM\system\currentcontrolset\enum\root\ms sstpminiport\0000[driver]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
    Queries value:
                                                    08002be10318}\0001\linkage[upperbind]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
                                                    HKLM \ system \ control \ wmi \ security [981f2d81-b1f3-11d0-mi] \ system \ control \ wmi \ system \
    Oueries value:
8dd7-00c04fc3358c1
   Queries value:
                                                    0000-00000000000001
    Queries value:
```

 $HKLM \setminus system \setminus current control set \setminus services \setminus wlansvc \setminus parameters [serviced llunload on stop]$ 

```
Queries value:
                                                                                                                                 HKLM\system\currentcontrolset\control\wmi\security[981f2d80-b1f3-11d0-
  8dd7-00c04fc3358c]
           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]
                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
          Oueries value:
 08002be10318}\0002[netcfginstanceid]
         Queries value:
                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  08002be10318}\0003[netcfginstanceid]
           Queries value:
                                                                                                                                 08002be10318}\0004[netcfginstanceid]
                                                                                                                                 Queries value:
  08002be10318}\0005[netcfginstanceid]
           Queries value:
                                                                                                                                 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]
                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
         Oueries value:
 08002be10318}\0009[netcfginstanceid]
          Queries value:
                                                                                                                                 HKLM \setminus system \setminus current control \\ \  \setminus \{4d36e972-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-e325-11ce-bfc1-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]
          Oueries value:
                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 08002be10318}\0012[netcfginstanceid]
                                                                                                                                 HKCR\clsid\{fc5eeaf6-2001-11df-adb9-f4ce462d9137}[]
          Oueries value:
                                                                                                                                HKCR\clsid\{fc5eeaf6-2001-11df-adb9-
          Queries value:
  f4ce462d9137}\inprocserver32[inprocserver32]
                                                                                                                                HKCR\clsid\{fc5eeaf6-2001-11df-adb9-f4ce462d9137}\ \ linprocserver 32[]
          Oueries value:
         Oueries value:
                                                                                                                                HKCR\clsid\{fc5eeaf6-2001-11df-adb9-
   f4ce462d9137}\inprocserver32[threadingmodel]
          Queries value:
                                                                                                                                 {\tt HKLM \setminus software \setminus microsoft \setminus wcmsvc[wlanminsignal strength]}
          Queries value:
                                                                                                                                 HKLM\software\microsoft\wcmsvc[wlanweaksignalmeasureinterval]
                                                                                                                                 {\it HKLM} \verb|\software\microsoft\wcmsvc[wlangoodsignalmeasureinterval]|
           Queries value:
           Oueries value:
                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  08002be10318}\0011[characteristics]
                                                                                                                                HKLM\system\currentcontrolset\control\wmi\security[082f46b6-01f6-4511-
          Queries value:
  9044-d83675f466371
         Queries value:
  HKLM\software\microsoft\wcmsvc\subscriptionmanager[servertimeretryperiod]
          Oueries value:
                                                                                                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  08002be10318}\0012[characteristics]
          Oueries value:
  HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
  fa9117f3e6f2}[]
          Queries value:
 HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{67d07935-283a-4791-8f8d-1864-1864, \ name \ name\ name \ 
  fa9117f3e6f2}[messagefilename]
         Oueries value:
HKLM \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus winevt \setminus publishers \setminus \{67d07935-283a-4791-8f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18f8d-18
  fa9117f3e6f2}[categorymessagefile]
         Oueries value:
 HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
  fa9117f3e6f2}[resourcefilename]
         Queries value:
 HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{67d07935-283a-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f8d-4791-8f
  fa9117f3e6f2}[parameterfilename]
           Queries value:
 HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
  fa9117f3e6f2}[helplink]
         Queries value:
  HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
  fa9117f3e6f2}[enabled]
         Oueries value:
 HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
 fa9117f3e6f2}[categorycount]
          Oueries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\c
 wcmsvc/operational[type]
          Queries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv
 wcmsvc/operational[enabled]
          Oueries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\micr
 wcmsvc/operational[filemax]
          Queries value:
 HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
 wcmsvc/operational[filecounter]
         Oueries value:
 HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi
 wcmsvc/operational[buffersize]
          Queries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv
 wcmsvc/operational[minbuffers]
          Queries value:
```

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/operational[maxbuffers]

Oueries value

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/operational[latency]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/operational[clocktype]

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - wcmsvc/operational[sidtype]$ 

Queries value:

 $\label{thm:hklm} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-wcmsvc/operational[level]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-wcmsvc/operational[controlguid]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/operational[maxsize]

Oueries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc urrentversion\winevt\channels\mbox{\sc microsoft-windows-wcmsvc/operational[maxsizeupper]} \\$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/operational[retention]

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - wcmsvc/operational \cite{loss} autobackuplog files \cite{loss}$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Queries value:

 $\label{thm:hammer} HKLM\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/operational[filterid]$ 

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc urrentversion\winevt\channels\mbox{\sc microsoft-windows-wcmsvc/operational[isolation]} \\$ 

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \microsoft-windows-wcmsvc/operational[owningpublisher]$ 

Queries value:

 $\label{thm:loss-twindows-wcmsvc/operational[channelaccess]} HKLM \software \microsoft-windows-wcmsvc/operational[channelaccess]$ 

Queries value:

 $HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - wcmsvc/diagnostic[type] \\$ 

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \microsoft-windows-wcmsvc/diagnostic[enabled]$ 

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - wcmsvc/diagnostic \mbox{[filemax]}$ 

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[buffersize]

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \ensuremath{\mbox{\mbox{$\rm Windows-wcmsvc/diagnostic[minbuffers]}} \\$ 

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[latency]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wind$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-wcmsvc/diagnostic[sidtype]$ 

Queries value:

 $\label{thm:hammels} HKLM\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-wcmsvc/diagnostic[level]$ 

Queries value:

 $\label{thm:hkk} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-wcmsvc/diagnostic \cite{thm:hkk} keywords \cite{thm:hkk} windows-wcmsvc/diagnostic \cite{thm:hkk} keywords \cite{thm$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[keywordsupper]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[controlguid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[maxsize]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ wcmsvc/diagnostic[maxsizeupper]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ wcmsvc/diagnostic[retention]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[autobackuplogfiles]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[file]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ wcmsvc/diagnostic[filterid]

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} windows \end{tabular} - \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} - \begin{tabular}{ll} HKLM \end{tabula$ wcmsvc/diagnostic[isolation]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ wcmsvc/diagnostic[owningpublisher]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ wcmsvc/diagnostic[channelaccess]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{89fe8f40-cdce-464e-8217-1946, \ next \ publishers \ \ \}$ 15ef97d4c7c3}[]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[messagefilename]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{89fe8f40-cdce-464e-8217-164e-82$ 15ef97d4c7c3}[categorymessagefile]

Oueries value:

15ef97d4c7c3}[resourcefilename]

Queries value:

15ef97d4c7c3}[parameterfilename]

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus publishers \setminus \{89fe8f40 - cdce - 464e - 8217 -$ 15ef97d4c7c3}[helplink]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{89fe8f40-cdce-464e-8217-164e-82$ 15ef97d4c7c3}[enabled]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[categorycount]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[type]

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows \ - crypto-part \ - crypto-par$ dpapi/operational[enabled] Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current \lor winevt \setminus channels \setminus microsoft \cdot windows \cdot crypto-properties of the software \setminus microsoft \cdot windows \cdot crypto-properties of the software \setminus microsoft \cdot windows \cdot crypto-properties of the software \setminus microsoft \cdot windows \cdot crypto-properties of the software \setminus microsoft \cdot windows \cdot crypto-properties of the software \cdot windows \cdot wind$ dpapi/operational[filemax] Oueries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-crypto-defined by the software \ microsoft-windows \ crypto-defined by the software \ microsoft-windows \ micr$ dpapi/operational[filecounter]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-property \ channels \ microsoft \ - windows \ - crypto-property \ - crypto$ dpapi/operational[buffersize]

Queries value:

 $\label{thm:local_equation} \begin{tabular}{ll} HKLM \label{thm:local_equation} \\ HKLM \label{thm:local_equation} \end{tabular} $$ HKLM \label{thm:local_equation} $$ HKLM \label{thm:local_eq$ dpapi/operational[minbuffers]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[maxbuffers]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[latency]

Oueries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-crypto-defined by the software \ microsoft-windows \ crypto-defined by the software \ microsoft-windows \ micr$ dpapi/operational[clocktype]

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows \ - crypto-part \ - crypto-par$ dpapi/operational[sidtype]

Oueries value:

 $HKLM \ software \ microsoft-windows \ - crypto-like \ microsoft-windows \ - crypto-like \$ dpapi/operational[level]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crvptodpapi/operational[controlguid]

Oueries value:

dpapi/operational[maxsize]

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows \ - crypto-part \ - crypto-par$ dpapi/operational[maxsizeupper]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[retention]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[autobackuplogfiles]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[file]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[isolation]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[owningpublisher]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[channelaccess]

Queries value:

 $\label{thm:local-microsoft-windows-crypto-def} HKLM \software \mbox{\sc crypto-depi/backupkeysvc[type]} \\$ 

Queries value:

 $\label{thm:local-microsoft-windows-crypto-def} HKLM \software \mbox{\sc crypto-depi/backupkeysvc[enabled]}$ 

Queries value:

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-crypto-dpapi/backupkeysvc[filecounter]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-crypto-dpapi/backupkeysvc[buffersize]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapai/backupkeys \circlescored local-property \circlescored local-p$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/backupkeys \cc[maxbuffers]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/backupkeys \cite{latency} \ \ \cite{latency} \ \cite{latency} \ \ \cite{latency} \ \cite$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-crypto-dpapi/backupkeysvc[sidtype]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapi/backupkeysvc[level]$ 

Queries value:

 $\label{thm:local-problem} HKLM \software \microsoft-windows-cryptodapi/backupkeysvc[controlguid]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapai/backupkeysvc[maxsize]$ 

Queries value:

 $\label{thm:local-microsoft-windows-crypto-def} HKLM \software \mbox{\sc crypto-depi/backupkeysvc[maxsizeupper]} \\$ 

Queries value:

 $\label{thm:hklm:software} HKLM \software \microsoft-windows-crypto-dpapi/backupkeysvc[retention]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/backupkeys \cite{local-prop} cauchy \cit$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapi/backupkeysvc[file]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapai/backupkeys \cite{thm:local-prop} literid]$ 

Queries value:

 $\label{thm:local_hammels} HKL^{M} software \verb|\microsoft| windows \verb|\currentversion| winevt\channels \verb|\microsoft| windows \verb|\crypto-dpapi| backupkeys vc[isolation]$ 

Queries value:

 $\label{thm:hklm:software} HKLM \software \microsoft-windows-cryptodapai/backupkeysvc[owningpublisher]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} Channels \label{lem:hklm} Winevt \label{lem:hklm} W$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/debug[type]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/debug[enabled]$ 

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/debug[filemax]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/debug[filecounter]

Oueries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-crypto-dpapi/debug[buffersize]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/debug[minbuffers]$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Hklm \label{lem:hklm} \label{lkm} \label{lk$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-crypto-dpapi/debug[latency]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/debug[clocktype]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-crypto-dpapi/debug[sidtype]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/debug[level]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \sincos of twindows \current version \winevt \channels \sincos of t-windows - crypto-dpapi/debug[controlguid]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapi/debug[maxsize]$ 

Queries value:

 $HKLM\$  software \microsoft \windows \current version \winevt \channels \microsoft - windows - cryptodebug [maxsizeupper]

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-crypto-dpapi/debug[retention]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-crypto-dpapi/debug[autobackuplogfiles]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/debug[file]

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-crypto-dpapi/debug[filterid]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapi/debug[isolation]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapi/debug[owningpublisher]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodpapi/debug[channelaccess]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-d5be7d52d6de\}[]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-d5be7d52d6de\} \ [message filename]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\mbox{$^9580d7dd-0379-4658-9870-d5be7d52d6de}[category messagefile]} \\$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-d5be7d52d6de\} \ [resource filename]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-d5be7d52d6de\} \ [parameter filename]$ 

Queries value:

Queries value

 $\label{thm:local_ham} $HKL_M \cap \exp\{\min(379-4658-9870-d564\}\} = \frac{1}{2} \left[ \exp\{\frac{1}{2} + \frac{1}{2} + \frac{1$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-d5be7d52d6de\} \ [category count]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[type]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} Windows \label{lem:hklm} winevt \label{lem:hklm} Windows \label{lem:hklm} winevt \$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} winevt \la$ 

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-wlandard \ microsoft-windows \$ autoconfig/operational[filecounter]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlandow$ autoconfig/operational[buffersize]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[minbuffers]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[maxbuffers]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlandow$ autoconfig/operational[latency]

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-wlandard \ microsoft-windows \$ autoconfig/operational[clocktype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[sidtype]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ -windows - winevt \ channels \ microsoft - windows - wlandard \ -windows - wlandard \ -win$ autoconfig/operational[level]

Queries value:

 $HKLM \ software \ microsoft\ windows \ current version \ winevt \ channels \ microsoft\ -windows\ -wlandard \ -w$ autoconfig/operational[controlguid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[maxsize]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[maxsizeupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[retention]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlandow$ autoconfig/operational[autobackuplogfiles]

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-wlandard \ microsoft-windows \$ autoconfig/operational[file]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[filterid]

Oueries value:

autoconfig/operational[isolation]

Oueries value:

 $HKLM \ software \ microsoft\ windows \ -windows - winevt\ -windows - windows - windo$ autoconfig/operational[owningpublisher]

Queries value:

 $HKLM \ software \ microsoft\ windows \ -windows - winevt\ -winevt\ -windows - winevt\ -winevt\ -winevt$ autoconfig/operational[channelaccess] Oueries value:

 $HKLM \verb|\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-wlandles \verb|\software\microsoft-windows\channels\chan$ autoconfig/diagnostic[type]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/diagnostic[enabled]

Queries value:

 $HKLM \ software \ microsoft \ windows \ -windows - winner \ than nels \ microsoft - windows - wlandows - winner \ than nels \ microsoft - windows - wlandows - winner \ than nels \ microsoft - winner \ micr$ autoconfig/diagnostic[filemax]

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-wlandard \ microsoft-windows \ winevt \ channels \ microsoft-windows \$ autoconfig/diagnostic[filecounter]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/diagnostic[buffersize]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ -winevt \ channels \ microsoft \ -windows \ -winevt \ -windows \ -windo$  $\verb"autoconfig/diagnostic[minbuffers]"$ 

Oueries value:

 $HKLM \ software \ microsoft\ windows \ current version \ winevt\ channels\ microsoft\ -windows\ -wlandard\ -wlandard\$ autoconfig/diagnostic[maxbuffers]

Queries value:

 $HKLM \ software \ microsoft\ windows \ -windows - winevt\ -winevt\ -windows - winevt\ -winevt\ -winevt$ autoconfig/diagnostic[latency]

Oueries value:

 $HKLM \verb|\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-wlandows \verb|\software\microsoft-windows\channels\microsoft-windows-wlandows \verb|\software\microsoft-windows\channels\microsoft-windows\channels\c$ autoconfig/diagnostic[clocktype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/diagnostic[sidtype]

Oueries value:

autoconfig/diagnostic[level]

Queries value:

 $HKLM \ software \ microsoft\ windows \ current version \ winevt \ channels \ microsoft\ -windows\ -wlandard \ -w$ autoconfig/diagnostic[keywordslower]

```
HKLM \ software \ microsoft\ windows \ current version \ winevt \ channels \ microsoft\ -windows\ -wlandard \ -w
autoconfig/diagnostic[keywordsupper]
       Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandow
autoconfig/diagnostic[controlguid]
      Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-
autoconfig/diagnostic[maxsize]
      Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-
autoconfig/diagnostic[maxsizeupper]
       Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandows-wlandow
autoconfig/diagnostic[retention]
       Queries value:
HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-wlandard \ microsoft-windows \
autoconfig/diagnostic[autobackuplogfiles]
      Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-
autoconfig/diagnostic[file]
      Oueries value:
autoconfig/diagnostic[filterid]
       Queries value:
HKLM \ software \ microsoft\ windows \ current version \ winevt \ channels \ microsoft\ -windows\ -wlandard \ -w
autoconfig/diagnostic[isolation]
       Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlan-
autoconfig/diagnostic[owningpublisher]
      Queries value:
HKLM \ software \ microsoft \ windows \ -windows \ -w
autoconfig/diagnostic[channelaccess]
       Oueries value:
                                                                                                        HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility
assistant\store[c:\windows\temp\toggleservice32.exe]
      Queries value:
                                                                                                      HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]
       Oueries value:
HKLM \verb|\system| current control set \verb|\services| tcpip \verb|\parameters[arpretry count]|
        Queries value:
        Oueries value:
                                                                                                        HKLM\system\currentcontrolset\services\tcpip\parameters[igmplevel]
       Queries value:
                                                                                                        HKLM\system\currentcontrolset\services\tcpip\parameters[igmpversion]
       Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableaddrmaskreply]
      Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \texttt{[disable task offload]}
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablebcastarpreply]
       Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledhcpmediasense]
       Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablemediasenseeventlog]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablemulticastforwarding]
      Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtudiscovery]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpuserfc1122urgentpointer]
       Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdataretransmissions]
        Queries value:
                                                                                                        HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
       Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcptimedwaitdelay]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpfinwait2delay]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtubhdetect]
       Queries value:
                                                                                                        HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [tcp1323 opts]
       Oueries value:
\label{lem:hklm} \verb|HKLM| system| current control set \verb|\services| tcpip| parameters [enable connection rate limiting]| | lem substitution of the system of
        Queries value:
                                                                                                      HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
       Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [qualifying destination threshold]
      Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationenabled]
      Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [ipautoconfiguration subnet]
      Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationmask]
       Queries value:
                                                                                                        HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
       Oueries value:
                                                                                                        HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [arpuse ether snap]
       Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[overridedefaultaddressselection]
```

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

Queries value: Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters[enableipautoconfigurationlimits]
55779daa70e9}[ipaddress]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[subnetmask1
   Oueries value:
55779daa70e9}[ipautoconfigurationaddress]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[ipautoconfigurationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[performrouterdiscovery]
   Queries value:
55779daa70e9}[defaultgateway]
   Oueries value:
55779daa70e9}[defaultgatewaymetric]
   Oueries value:
55779daa70e9}[solicitationaddressbcast]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[usezerobroadcast]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[typeofinterface]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[mtu]
   Oueries value:
55779daa70e9}[interfacemetric]
55779daa70e9}[tcpackfrequency]
   Queries value:
55779daa70e9}[tcpdelackticks]
   Oueries value:
\label{thm:local-condition} \label{thm:local-condition} HKCU \software \mbox{\sc microsoft} \windows \sc urrent version \end{\sc version} explorer \sc user as sist \sc urrent version \end{\sc version} \sc urrent version \sc urrent version \sc urrent version \sc urrent version \end{\sc version} \sc urrent version \sc urrent version \sc urrent version \sc urrent version \end{\sc version} \sc urrent version \s
9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
                                                    HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
   Queries value:
   Oueries value:
                                                    HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
   Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\browser[providerguid]
                                                    HKLM\system\currentcontrolset\services\sppsvc[objectname]
    Queries value:
   Queries value:
                                                    HKLM\system\currentcontrolset\services\sppsvc[imagepath]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\sppsvc[wow64]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
                                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
   Oueries value:
20[profileimagepath]
   Oueries value:
                                                    HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
   Oueries value:
                                                    HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\sppsvc[environment]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\sppsvc[startprotected]
   Queries value:
                                                    HKLM\software\microsoft\windows
nt\currentversion\compatibility32[sppsvc]
                                                    Queries value:
a5f9-f2bdfea0f156]
                                                    Queries value:
protection platform service[providerguid]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-
f2bdfea0f156}[1
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{e23b33b0-c8c9-472c-a5f9-microsoft\} \ windows \ version \ versio
f2bdfea0f156}[messagefilename]
   Queries value:
f2bdfea0f156}[categorymessagefile]
   Oueries value:
f2bdfea0f156}[resourcefilename]
   Queries value:
f2bdfea0f156}[parameterfilename]
   Oueries value:
HKLM \ software \ `microsoft \ `windows \ `current version \ `winevt \ publishers \ `\{e23b33b0-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9-c8c9-472c-a5f9
f2bdfea0f156}[helplink]
   Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-
f2bdfea0f156}[enabled]
```

```
f2bdfea0f156}[categorycount]
                          HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\software| protection platform[inactivity shutdown delay]| \\
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[keeprunningthresholdmins]
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\softwareprotectionplatform[tokenstore]
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1[]
 Oueries value:
 Oueries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10[]
 Oueries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11[]
 Oueries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12[]
 Queries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13[]
 Queries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14[]
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15[]
  Queries value:
                          HKLM\system\currentcontrolset\services\wsearch[objectname]
  Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\winmgmt[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\wscsvc[objectname]
                          HKLM\system\currentcontrolset\services\wscsvc[requiredprivileges]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\wscsvc\parameters[servicedll]
 Queries value:
HKLM\system\currentcontrolset\services\wscsvc\parameters[servicemanifest]
  Queries value:
                          \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ wscsvc \+ parameters [service main]
  Oueries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16[]
  Queries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17[]
 Queries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18[]
  Queries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19[]
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2[]
  Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-
809b-2a87b70881f8]
                          HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-
 Queries value:
8539-9230a44081a5]
 Oueries value:
                          HKLM\software\microsoft\security center\svc[vistasp1]
 Oueries value:
                          {\tt HKLM \setminus software \setminus microsoft \setminus security \ center \setminus svc[antivirus override]}
                          HKLM\software\microsoft\security center\svc[antispywareoverride]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\security center\svc[firewalloverride]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
 Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
  Queries value:
 Oueries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
 Oueries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Oueries value:
                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
                          HKCR \ appid \ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\}[]
 Oueries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
 Oueries value:
 Oueries value:
                          HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [service parameters]
 Queries value:
                          HKCR \ appid \ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [runas]
  Queries value:
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20[]
 Queries value:
                          \label{locality} HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}[activateatstorage]}
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[rotflags]
  Oueries value:
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appidflags]
                          \label{locality} \mbox{HKCR\appid\8bc3f05e-d86b-11d0-a075-00c04fb68820}[launch permission]
 Queries value:
                          HKLM\software\microsoft\ole[legacyauthenticationlevel]
 Oueries value:
 Oueries value:
                          {\tt HKLM \setminus software \setminus microsoft \setminus ole[legacyimpersonationlevel]}
 Oueries value:
                          HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [authenticationlevel]
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[remoteservername]
 Queries value:
 Oueries value:
                          HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [srptrustlevel]
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}[preferredserverbitness]
                          HKCR \land ppid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [loadusersettings]
  Queries value:
                          HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Queries value:
                          HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
  Queries value:
                          Oueries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
 Queries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-
 Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
  Oueries value:
                          HKCR \ interface \ \{d4781cd6-e5d3-44df-ad94-930efe48a887\} \ proxystubclsid32[]
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:
                          HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
                          HKCR \ interface \ \{9556dc99-828c-11cf-a37e-00aa003240c7\} \ \ proxystubclsid32[]
  Queries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
  Oueries value:
 Queries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21[]
  Queries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-
 Oueries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\wbem\cimom[processid]
  Queries value:
                          HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[contextlimit]
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[objectlimit]
  Queries value:
                          HKLM\software\microsoft\wbem\cimom[identifierlimit]
                          HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
  Queries value:
```

```
Queries value:
                                                                                                                    HKCR\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[inprocserver32]
                                                                                                                     HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprocserver32[]
         Queries value:
        Queries value:
                                                                                                                    HKCR\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[threadingmodel]
                                                                                                                   HKLM\software\microsoft\com3[gipactivitybypass]
       Oueries value:
                                                                                                                    HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\proxystubclsid32[]
        Oueries value:
                                                                                                                    HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}[]
        Oueries value:
                                                                                                                    HKCR\clsid\{71285c44-1dc0-11d2-b5fb-
       Oueries value:
00104b703efd}\inprocserver32[inprocserver32]
                                                                                                                    HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32[]
         Queries value:
        Queries value:
                                                                                                                   HKCR\clsid\{71285c44-1dc0-11d2-b5fb-
00104b703efd}\inprocserver32[threadingmodel]
         Queries value:
                                                                                                                    HKCR\interface[interfacehelperdisableall]
                                                                                                                     HKCR\interface[interfacehelperdisableallforole32]
         Queries value:
                                                                                                                     HKCR\interface[interfacehelperdisabletypelib]
         Oueries value:
        Queries value:
                                                                                                                     HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                                                                                                                   HKCR\interface\{00020400-0000-0000-c000-
       Queries value:
00000000046}[interfacehelperdisableallforole321
                                                                                                                    ...
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22[]
        Oueries value:
       Queries value:
                                                                                                                    HKCR\interface\{7c857801-7381-11cf-884d-
00aa004b2e24}[interfacehelperdisabletypelib]
         Queries value:
                                                                                                                     HKCR\interface\{7c857801-7381-11cf-884d-
00aa004b2e24}[interfacehelperdisableall]
                                                                                                                     HKCR\interface\{7c857801-7381-11cf-884d-
         Queries value:
00aa004b2e24}[interfacehelperuser]
        Queries value:
                                                                                                                   HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
         Oueries value:
                                                                                                                    HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
        Queries value:
                                                                                                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
                                                                                                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
        Queries value:
        Oueries value:
                                                                                                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
                                                                                                                    HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
        Oueries value:
                                                                                                                     HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
        Queries value:
        Queries value:
                                                                                                                     HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}[]
        Queries value:
                                                                                                                     HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23[]
                                                                                                                     HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24[]
         Queries value:
        Oueries value:
                                                                                                                     HKCR\clsid\{bfe18e9c-6d87-4450-b37c-
e02f0b373803}\inprocserver32[inprocserver32]
                                                                                                                     HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25[]
        Queries value:
        Queries value:
                                                                                                                     HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32[]
                                                                                                                    HKCR\clsid\{bfe18e9c-6d87-4450-b37c-
       Oueries value:
e02f0b373803}\inprocserver32[threadingmodel]
        Oueries value:
9d55-7b8e7f157091}[category]
       Queries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ expl
9d55-7b8e7f157091}[name]
        Queries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lkklm} White \label{lkklm} White \label{lkklm} White \label{
9d55-7b8e7f157091}[parentfolder]
       Oueries value:
9d55-7b8e7f157091}[description]
       Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[relativepath]
        Queries value:
                                                                                                                     HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26[]
        Queries value:
                                                                                                                     HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27[]
        Queries value:
                                                                                                                     HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28[]
        Queries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f1b32785-6fba-4fcf-10cf \ folder descriptions \ \ f1b32785-6fba-4fcf-10cf \ folder \ fol
9d55-7b8e7f157091}[parsingname]
       Oueries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ e
9d55-7b8e7f157091}[infotip]
       Queries value:
HKLM \label{lem:hklm} In the latest and the lates
9d55-7b8e7f157091}[localizedname]
        Oueries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ expl
9d55-7b8e7f157091}[icon]
         Queries value:
\label{thm:local-continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 1532785-6 fba-4 fcf-4 fc
9d55-7b8e7f157091}[security]
       Queries value:
9d55-7b8e7f157091}[streamresource]
       Oueries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ e
9d55-7b8e7f157091}[streamresourcetype]
        Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localredirectonly]
       Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f1b32785-6fba-4fcf-10cf \ folder descriptions \ \ f1b32785-6fba-4fcf-10cf \ folder \ fol
9d55-7b8e7f157091}[roamable]
```

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ e$ 9d55-7b8e7f157091}[precreate]

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ e$ 9d55-7b8e7f157091}[stream]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f1b32785-6fba-4fcf-10cf \ folder descriptions \ \ f1b32785-6fba-4fcf-10cf \ folder \ fol$ 9d55-7b8e7f157091}[publishexpandedpath]

Oueries value:

9d55-7b8e7f157091}[attributes]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]

9d55-7b8e7f157091}[initfolderhandler]

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29[] Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3[] Oueries value:

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

folders[local appdata]

Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30[] Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31[] HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32[] Oueries value:

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} with the lem \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lklm} With \labe$ 9afe-ea3317b67173}[category]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[name]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]

Oueries value:

9afe-ea3317b67173}[description]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1200' \ explorer \ 'folder descriptions' \ 'folder des$ 9afe-ea3317b67173}[relativepath]

Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33[] HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4[] Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Oueries value:

9afe-ea3317b67173}[infotip]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[localizedname]

Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5[] Queries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6[] HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7[] Oueries value: Oueries value:

9afe-ea3317b67173}[icon]

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8[] Oueries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9[] Oueries value: Queries value:

9afe-ea3317b67173}[security]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[streamresource]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1200' \ explorer \ 'folder descriptions' \ 'folder des$ 9afe-ea3317b67173}[roamable]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[precreate]

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[stream]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[initfolderhandler] Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[auoptions] Queries value: HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update[autoinstallminorupdates]  $\label{lem:hklmsoftware} \verb+MKLM\+ software \verb+\microsoft+ windows \verb+\currentversion+ window supdate \verb+\auto+ auto+ windows \verb+\currentversion+ windows \verb+\cu$ Oueries value: update[includerecommendedupdates] Queries value: update[elevatenonadmins] Queries value: update[configver] Queries value: 3937643e37a3}[1 Oueries value: 3937643e37a3}[messagefilename] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[categorymessagefile] Queries value:  $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{4ee76bd8-3cf4-44a0-a0ac-4bd8-3cf4-44a0-a0ac-4bd8-3cf4-44a0-a0ac-4bd8-3cf4-44a0-a0ac-4bd8-3cf4-4bd8-3c$ 3937643e37a3}[resourcefilename] Queries value: 3937643e37a3}[parameterfilename] Queries value: 3937643e37a3}[helplink] Oueries value:  $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{4ee76bd8-3cf4-44a0-a0ac-4bd8-3cf4-44a0-a0ac-4bd8-3cf4-44a0-a0ac-4bd8-3cf4-44a0-a0ac-4bd8-3cf4-4bd8-3c$ 3937643e37a3}[enabled] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[categorycount] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/operational[type] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/operational[enabled] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/operational[filemax] Oueries value:  $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ codeintegrity/operational[filecounter] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/operational[buffersize] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/operational[minbuffers] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/operational[maxbuffers] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/operational[latency] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/operational[clocktype] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/operational[sidtype] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/operational[level] Queries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ codeintegrity/operational[controlguid] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/operational[maxsize] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/operational[maxsizeupper] Queries value:  $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the substitution of the subs$ codeintegrity/operational[retention] Oueries value: HKLM\software\microsoft\security center[cval] Oueries value: HKLM\system\currentcontrolset\services\eventlog\application\securitycenter[providerguid]

HKLM\software\microsoft\windows\currentversion\policies\system[enablelua] Queries value:

HKLM\software\microsoft\windows\currentversion\policies\system[consentpromptbehavioradmin] Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

codeintegrity/operational[autobackuplogfiles]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the substitution of the subs$ codeintegrity/operational[file]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/operational[filterid]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ codeintegrity/operational[isolation]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/operational[owningpublisher]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/operational[channelaccess]

Queries value:

HKLM\system\currentcontrolset\services\wscsvc\parameters[servicedllunloadonstop] Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[type]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-displayer-based and the property of th$ codeintegrity/verbose[enabled]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/verbose[filemax]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/verbose[filecounter]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[buffersize]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[minbuffers]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/verbose[maxbuffers]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[latency]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[clocktype]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ codeintegrity/verbose[sidtype] Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/verbose[level]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ 

codeintegrity/verbose[keywordslower] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

codeintegrity/verbose[keywordsupper] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

codeintegrity/verbose[controlguid]

Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/verbose[maxsize]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/verbose[maxsizeupper]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/verbose[retention]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ codeintegrity/verbose[autobackuplogfiles]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ codeintegrity/verbose[file]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ codeintegrity/verbose[filterid]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ codeintegrity/verbose[isolation]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[owningpublisher]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowscodeintegrity/verbose[channelaccess]

HKLM\software\microsoft\windows Oueries value:

 $nt \verb|\currentversion| software protection platform \verb|\plugins| modules \verb|\179b8a65-b0f6-41d9-acea-def| and the platform \verb|\plugins| modules \verb|\protection| and the platform and th$ 12006ef9b32a[manifestfile]

```
HKLM\software\microsoft\windows
           Oueries value:
 nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
 12006ef9b32a[pluginfile]
           Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform \verb|plugins\modules\c42d83ff-5958-4af4-a0dd-1000| and the control of the con
ba02fed39662[manifestfile]
           Oueries value:
                                                                                                                                                            HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| modules \verb|\c42d83ff-5958-4af4-a0dd-10| deleta a software protection platform \verb|\plugins| modules modul
ba02fed39662[pluginfile]
         Oueries value:
                                                                                                                                                           HKLM\software\microsoft\windows
 nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/activedirectory/1.0[moduleid]| | the property of the property of
           Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 \verb|nt\currentversion\software| protection platform | plugins objects of the light 
            Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/bios/4.0[is service]| |
           Oueries value:
                                                                                                                                                            HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/flags/1.0[module id]| | the first term of the following protection of the following platform of the following platform of the first term of the following platform of the following platform of the first term of the first
                                                                                                                                                           HKLM\software\microsoft\windows
           Queries value:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[moduleid]
                                                                                                                                                            HKLM\software\microsoft\windows
           Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[moduleid]
         Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt \verb|\colored | learned | nt \verb|\colored | learned | le
                                                                                                                                                            HKLM\software\microsoft\windows
           Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[moduleid]
           Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
Queries value:
                                                                                                                                                           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[moduleid]
                                                                                                                                                           HKLM\software\microsoft\windows
         Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
                                                                                                                                                          HKLM\software\microsoft\windows
         Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[moduleid]
         Queries value:
                                                                                                                                                           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[moduleid]
         Queries value:
                                                                                                                                                           HKLM\software\microsoft\windows
Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/action/vlactivate/1.0[moduleid]| and the province of the property of the property of the province of the property of the
           Oueries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[moduleid]
                                                                                                                                                           HKLM\software\microsoft\windows
           Queries value:
nt \verb|\colored| restriction r
                                                                                                                                                           HKLM\software\microsoft\windows
         Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[moduleid]
           Oueries value:
                                                                                                                                                            HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/collector/kms/1.0[moduleid]| | the province of the p
           Oueries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt\current version\software protection platform\plugins\objects\mbox{\sc spp/licenseacquisition/payloadhandler/eul/1.0[moduleid]}
                                                                                                                                                            HKLM\software\microsoft\windows
           Queries value:
nt \verb|\colored | line 
            Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft:spp/licenseacquisition| payload handler/pkc/1.0[moduleid] | 
           Oueries value:
                                                                                                                                                           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[moduleid]
                                                                                                                                                          HKLM\software\microsoft\windows
         Queries value:
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/payloadhandler/spc/1.0[moduleid]|
         Queries value:
                                                                                                                                                           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[moduleid]
         Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[moduleid]
            Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
           Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
 nt\current version \colored by the continuous and the continuous continuous and the continuous continuous continuous and the continuous continuous continuous continuous and the continuous cont
                                                                                                                                                            HKLM\software\microsoft\windows
           Queries value:
HKLM\software\microsoft\windows
         Queries value:
\verb|nt\currentversion| software protection platform \verb|plugins\objects| msft: spp/windows functionality/agent/7.0[isservice]| | the province of the protection of the protectio
           Oueries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
                                                                                                                                                            HKLM\software\microsoft\windows
           Oueries value:
nt \verb|\colored| returned in r
            Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/flags/1.0[is service]| | the property of the pr
           Oueries value:
                                                                                                                                                           HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/hwid/4.0[is service]|
                                                                                                                                                           HKLM\software\microsoft\windows
         Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[isservice]
                                                                                                                                                          HKLM\software\microsoft\windows
         Oueries value:
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/pkey/2005[isservice]| | the property of the
         Oueries value:
                                                                                                                                                          HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform \verb|plugins\objects\msft:rm/algorithm/pkey/2009[isservice]| |
           Oueries value:
                                                                                                                                                           HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[isservice]
                                                                                                                                                           HKLM\software\microsoft\windows
           Queries value:
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/vmd/1.0[is service]| | the first term of the following terms of the following terms of the first terms o
           Queries value:
                                                                                                                                                            HKLM\software\microsoft\windows
```

```
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/volume/1.0[isservice]| | the latest theorem \verb|\plugins| objects 
                                                                                                             HKLM\software\microsoft\windows
nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft:spp/action/create process/1.0[isservice]| and the protection of the protection
        Queries value:
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[isservice]
                                                                                                            HKLM\software\microsoft\windows
       Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[isservice]
       Oueries value:
                                                                                                            HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/action/vlactivate/1.0[isservice]|
       Oueries value:
                                                                                                            HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/actionscheduler/1.0[isservice]| |
                                                                                                            HKLM\software\microsoft\windows
        Queries value:
 nt\current version\software protection platform\plugins\objects\nsft: spp/apihandler/object/active directory publisher/1.0[isservice]
                                                                                                            HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[isservice]
        Oueries value:
                                                                                                             HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/collector/kms/1.0[is service]|
                                                                                                            HKLM\software\microsoft\windows
       Queries value:
nt \verb|currentversion| software protection platform \verb| plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects \verb| objects acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects acquisition/payload handler/eul/1.0[isservice]| | the plugins \verb| objects acquisition/payload handler/eul/1.0[isservice]| | the plugins objects acquisition handler/eul/1.0[isservice]| | the plugins objects acquisiti
                                                                                                            HKLM\software\microsoft\windows
       Oueries value:
nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft:spp/licenseacquisition| payload handler/pa/1.0[isservice]| and the property of t
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
nt \verb|\color= | nt \verb
                                                                                                            HKLM\software\microsoft\windows
        Queries value:
nt \verb|currentversion| software protection platform \verb| plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| msft: spp/license acquisition/payload handler/rac/1.0[isservice]| | the plugins \verb| objects \verb| o
                                                                                                            HKLM\software\microsoft\windows
nt \verb|currentversion| software protection platform \verb| plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| msft:spp/license acquisition/payload handler/spc/1.0[is service]| and the plugins \verb| objects \verb| ob
                                                                                                            HKLM\software\microsoft\windows
       Queries value:
nt \verb|\current version| software protection platform software protection platform software protection platform software platform software platform software protection platform software p
                                                                                                            HKLM\software\microsoft\windows
       Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkev[isservice]
                                                                                                            HKLM\software\microsoft\windows
       Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[isservice]
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[isservice]
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
nt \verb|currentversion| software protection platform \verb| plugins \verb| objects \verb| msft: spp/volume/services/kms/activation info/1.0[isservice]| | the property of t
        Queries value:
                                                                                                            HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[kmshostconfig]
        Oueries value:
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[enabletestvolumeintervals]
                                                                                                            HKLM\software\microsoft\windows
        Queries value:
nt\currentversion\softwareprotectionplatform[vlactivationinterval]
                                                                                                            HKLM\software\microsoft\windows
       Oueries value:
nt\currentversion\softwareprotectionplatform[vlrenewalinterval]
       Oueries value:
                                                                                                            HKLM\software\microsoft\windows
\verb|nt\currentversion\software| protection platform[action list]|
       Oueries value:
 HKLM\software\microsoft\windows\currentversion\sidebyside[publisherpolicychangetime]
                                                                                                             HKLM\software\microsoft\windows
         Oueries value:
nt\currentversion\softwareprotectionplatform[cachestore]
         Queries value:
                                                                                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version [digital product id 4]
         Queries value:
                                                                                                             HKLM\system\setup\status[auditboot]
        Oueries value:
                                                                                                             HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[hardwareid]
        Oueries value:
                                                                                                            HKLM\svstem\currentcontrolset\enum\acpi\pnp0a03\0ſcompatibleids1
        Queries value:
Oueries value:
HKLM \setminus system \setminus current control set \\ \setminus enum \setminus pci \setminus ven\_8086 \\ \& dev\_1237 \\ \& subsys\_00000000 \\ \& rev\_02 \\ \setminus 38.267 \\ a616a \\ \& 18.00 \\ [compatible ids]
        Queries value:
HKLM \ system \ current control set \ enum \ pci \ ven\_8086\& dev\_7000\& subsys\_00000000\& rev\_00 \ 3\&267a616a\&1\&08 \ [hardwareid]
        Queries value:
HKLM \setminus system \setminus current control set \\ \setminus enum \setminus pci \setminus ven\_8086 \\ \& dev\_7000 \\ \& subsys\_00000000 \\ \& rev\_00 \\ \setminus 38267 \\ a616 \\ a818 \\ \& 08[compatible ids]
                                                                                                             HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[hardwareid]
         Queries value:
         Queries value:
HKLM \setminus system \setminus current control set \setminus enum \setminus acpi \setminus pnp0303 \setminus 4\&e03a844\&0 [compatible ids]
                                                                                                            HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[hardwareid]
        Queries value:
        Queries value:
HKLM\svstem\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0\compatibleids1
                                                                                                            Queries value:
        Oueries value:
Queries value:
                                                                                                             Oueries value:
 HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[compatibleids]
Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[hardwareid]
       Queries value:
        Queries value:
HKLM\svstem\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0\compatibleids1
                                                                                                            Oueries value:
        Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[compatibleids]
        Oueries value:
HKLM \setminus system \setminus current control set \setminus enum \setminus pci \setminus ven\_8086 \& dev\_7111 \& subsys\_00000000 \& rev\_01 \setminus 3 \& 267a616a \& 1 \& 09 [hardware id]
        Queries value:
Queries value:
```

```
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[hardwareid]
HKLM \setminus system \setminus current control set \setminus enum \setminus pciide \setminus idechannel \setminus 4\&20064 fa2\&0\&0 [compatible ids]
  Queries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_
                                                                                                                     1.0.7.3 \5&34baf594&0&0.0.0[hardwareid]
  Oueries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi
                                                                                                                      1.0.7.3 \5&34baf594&0&0.0.0[compatibleids]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus enum \setminus pciide \setminus idechannel \setminus 4\&20064 fa2\&0\&1 [hardwareid]
  Oueries value:
HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\softwareprotectionplatform[licstatusarray]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[policyvaluesarray]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[hasooberun]
                                   HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}[]
  Queries value:
                                   HKCR\clsid\{88d96a06-f192-11d4-a65f-
  Queries value:
0040963251e5}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Oueries value:
  Oueries value:
                                   HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}[]
  Queries value:
                                   HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value:
                                    HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[servicesessionid]
                                   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\softwareprotectionplatform[logcontext]
                                   HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]
  Oueries value:
                                   HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
  Oueries value:
73e6154572dd}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\productoptions[productpolicy]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\parameters[servicedllunloadonstop]
                                   HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]
  Queries value:
                                   HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
  Oueries value:
323e85a1ce84}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]
  Oueries value:
  Oueries value:
                                   HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32[threadingmodel]
  Queries value:
                                   833b-323e85a1ce841
                                    HKLM\software\policies\microsoft\internet
  Queries value:
explorer\security[disablesecuritysettingscheck]
  Queries value:
                                   HKLM\software\policies\microsoft\internet
explorer\security[disablefixsecuritysettings]
                                   HKCU\software\microsoft\internet
  Queries value:
explorer\security[disablefixsecuritysettings]
                                   HKLM\software\microsoft\internet
  Oueries value:
explorer\security[disablefixsecuritysettings]
  Oueries value:
                                    HKLM\svstem\currentcontrolset\services\wscsvc[tvpe]
  Queries value:
                                    HKLM\system\currentcontrolset\services\wscsvc[start]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\wscsvc[errorcontrol]
  Queries value:
                                    HKLM\system\currentcontrolset\services\wscsvc[tag]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\wscsvc[dependonservice]
  Queries value:
                                    HKLM\system\currentcontrolset\services\wscsvc[dependongroup]
  Queries value:
                                    HKLM\system\currentcontrolset\services\wscsvc[group]
  Queries value:
                                    HKLM\software\microsoft\security center[autoupdatedisablenotify]
  Queries value:
                                    HKLM\software\microsoft\security center[internetsettingsdisablenotify]
                                    HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.106[checksetting]
                                   HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.101[checksetting]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.103[checksetting]
  Oueries value:
                                   \label{lem:hkcu} \verb+KCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100[checksetting]
  Queries value:
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.102[checksetting]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.104[checksetting]
                                   HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]
  Queries value:
  Queries value:
                                   HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[]
  Oueries value:
                                   HKCR\clsid\{ca236752-2e77-4386-b63b-
  Oueries value:
0e34774a413d}\inprocserver32[threadingmodel]
  Oueries value:
                                   HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:
                                    HKLM \ system \ current control \ wmi \ security [a0ef609d-0a14-424c-mi] \ a0ef609d-0a14-424c-mi] \ a0ef609d-0a14-mi] \ a0ef
9270-3b2691a0a3941
```

HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-

Queries value:

86ba-948b704162201

```
Queries value:
                                                                                                                                           HKLM\software\microsoft\windows\windows error reporting[disabled]
                                                                                                                                           HKCU\software\microsoft\windows\windows error reporting[disabled]
            Queries value:
                                                                                                                                           HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
            Queries value:
                                                                                                                                           HKCR\clsid\{88d96a05-f192-11d4-a65f-
          Queries value:
  0040963251e5}\inprocserver32[inprocserver32]
                                                                                                                                         HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]
          Oueries value:
          Oueries value:
                                                                                                                                          HKCR\clsid\{88d96a05-f192-11d4-a65f-
 0040963251e5}\inprocserver32[threadingmodel]
                                                                                                                                          HKCU\software\microsoft\windows\currentversion\action
         Queries value:
  center \verb|\checks|{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}|.check.100[checksetting]|
          Queries value:
                                                                                                                                          HKCU\software\microsoft\windows\windows error
  reporting[lastqueuepestertime]
                                                                                                                                           HKLM\software\microsoft\windows\windows error
          Queries value:
  reporting[queuepesterinterval]
                                                                                                                                          HKCU\software\microsoft\windows\windows error
          Queries value:
  reporting[queuepesterinterval]
         Queries value:
                                                                                                                                         HKCU\software\microsoft\windows\currentversion\action
 center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting]
                                                                                                                                         HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}[]
         Queries value:
                                                                                                                                         HKCR\clsid\{c8e6f269-b90a-4053-a3be-
          Oueries value:
  499afcec98c4}\inprocserver32[inprocserver32]
                                                                                                                                         HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
          Queries value:
          Oueries value:
                                                                                                                                         HKCR\clsid\{c8e6f269-b90a-4053-a3be-
  499afcec98c4}\inprocserver32[threadingmodel]
                                                                                                                                         HKCU\software\microsoft\windows\currentversion\action
          Oueries value:
  center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4\}.check.0[checksetting]
                                                                                                                                         HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}[]
                                                                                                                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-
            Queries value:
   f0aa6db5d4bc}\inprocserver32[inprocserver32]
          Queries value:
                                                                                                                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[]
                                                                                                                                         HKCR\clsid\{088e8dfb-2464-4c21-bad2-
          Queries value:
   f0aa6db5d4bc}\inprocserver32[threadingmodel]
                                                                                                                                         HKLM\software\policies\microsoft\windows\system[enablesmartscreen]
          Oueries value:
          Oueries value:
 HKLM\software\microsoft\windows\currentversion\explorer[smartscreenenabled]
         Queries value:
                                                                                                                                         HKCU\software\microsoft\windows\currentversion\action
 center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
            Queries value:
                                                                                                                                           HKCR\clsid\d26de5c1-c061-43f7-9c40-7517526cf1c1\[]
                                                                                                                                          HKCR\clsid\{d26de5c1-c061-43f7-9c40-
  7517526cf1c1}\inprocserver32[inprocserver32]
         Queries value:
                                                                                                                                         HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[]
          Queries value:
                                                                                                                                          HKCR\clsid\{d26de5c1-c061-43f7-9c40-
 7517526cf1c1}\inprocserver32[threadingmodel]
         Oueries value:
  HKCU\software\microsoft\windows\currentversion\startupnotify[enablestartupappnotification]
          Oueries value:
                                                                                                                                          HKCU\software\microsoft\windows\currentversion\action
  center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1\}.check.0[checksetting]
         Oueries value:
                                                                                                                                          HKCU\software\microsoft\windows\currentversion\action
  center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
            Oueries value:
 \label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$}$-windows-$} \noindent \
 windowsbackup/actioncenter[type]
          Queries value:
  HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
 windowsbackup/actioncenter[enabled]
          Queries value:
 HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
 windowsbackup/actioncenter[filemax]
          Oueries value:
 HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi
 windowsbackup/actioncenter[filecounter]
          Queries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\c
 windowsbackup/actioncenter[buffersize]
 HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat
 windowsbackup/actioncenter[minbuffers]
          Queries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\c
 windowsbackup/actioncenter[maxbuffers]
         Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
 windowsbackup/actioncenter[latency]
            Queries value:
 \label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$}$-windows-$} \noindent \
 windowsbackup/actioncenter[clocktype]
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv
 windowsbackup/actioncenter[sidtype]
         Queries value:
 HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
 windowsbackup/actioncenter[level]
         Oueries value:
 HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind
 windowsbackup/actioncenter[controlguid]
          Oueries value:
 HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv
 windowsbackup/actioncenter[maxsize]
 HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind
```

windowsbackup/actioncenter[maxsizeupper]  $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the substitution of the subs$ windowsbackup/actioncenter[retention] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswindowsbackup/actioncenter[autobackuplogfiles] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ windowsbackup/actioncenter[file] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ windowsbackup/actioncenter[filterid] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswindowsbackup/actioncenter[isolation] Queries value:  $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ windowsbackup/actioncenter[owningpublisher] Oueries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ windowsbackup/actioncenter[channelaccess] Oueries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[] Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[inprocserver32] HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[] Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[threadingmodel]  $\label{lem:hkcu} \verb+KCU\software\microsoft\windows\currentversion\action$ Oueries value: center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018\}.check.100[checksetting] HKCU\software\microsoft\windows\currentversion\action Oueries value: center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101[checksetting] Oueries value: HKCU\software\microsoft\windows\currentversion\action  $center \verb|\providers| eventlog \verb|\dab69a6a-4d2a-4d44-94bf-e0091898c881| [lastknown state]|$ Oueries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ networkaccessprotection/whc[type] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ networkaccessprotection/whc[enabled] Queries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - winevt \cdot channels \setminus microsoft - windows - winevt \cdot channels \setminus microsoft - windows - winevt \cdot channels \cdot microsoft - winevt \cdot channels \cdot microsoft - windows - winevt \cdot channels \cdot microsoft - windows - winevt \cdot channels \cdot microsoft - winevt \cdot channels \cdot channels \cdot channels \cdot micr$ networkaccessprotection/whc[filemax] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[filecounter] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[buffersize] Oueries value:  $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$}$-windows-$} \noindent \$ networkaccessprotection/whc[minbuffers] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[maxbuffers] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[latency] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ networkaccessprotection/whc[clocktype] Queries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ networkaccessprotection/whc[sidtype]  $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ networkaccessprotection/whc[level] Oueries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\channels\channels\channels\channels\channel\chan$ networkaccessprotection/whc[controlguid] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[maxsize] Queries value:  $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$}$-windows-$} \noindent \$ networkaccessprotection/whc[maxsizeupper]  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ networkaccessprotection/whc[retention] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[autobackuplogfiles] Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ networkaccessprotection/whc[file] Oueries value:  $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ networkaccessprotection/whc[filterid]

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ 

networkaccessprotection/whc[isolation]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the second content of the second c$ networkaccessprotection/whc[owningpublisher]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[channelaccess]

HKCU\software\microsoft\windows\currentversion\action Oueries value:

center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881\}.check.100[checksetting] Oueries value: HKCU\software\microsoft\windows\currentversion\action

center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate] Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-windo$ defender/whc[type]

Queries value:

 $HKLM \ software \ microsoft\ windows\ -windows\ -windo$ defender/whc[enabled]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[filemax]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[filecounter]

Queries value:

 $HKLM \ software \ microsoft\ windows\ -windows\ -windo$ defender/whc[buffersize]

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[minbuffers]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-windo$ defender/whc[maxbuffers]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[latency]

Queries value:

 $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ windows\ -windows$ defender/whc[clocktype]

 $HKLM \ software \ microsoft\ windows\ -windows\ -windo$ defender/whc[sidtype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[level]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[controlguid]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ windows \ described a property \ described \ described a property \ described \ described a property \ described \ desc$ defender/whc[maxsize]

Queries value:

 $HKLM \ software \ microsoft\ windows\ -windows\ -windo$ defender/whc[maxsizeupper] Oueries value:

 $HKLM \verb|\software\microsoft-windows-windows| winevt \verb|\channels\microsoft-windows-windows| winevt \verb|\channels\microsoft-windows-windows| winevt \verb|\channels\microsoft-windows-windows| winevt \verb|\channels\microsoft-windows-windows| winevt \verb|\channels\microsoft-windows-windows-windows| winevt \verb|\channels\microsoft-windows-windows-windows-windows| winevt \verb|\channels\microsoft-windows-window-windows-window-win$ defender/whc[retention]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[autobackuplogfiles]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[file]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -windows \ -windows$ defender/whc[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[isolation]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc[owningpublisher]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ windows \ described a property \ described \ described a property \ described \ described a property \ described \ desc$ defender/whc[channelaccess]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action$ Queries value: center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78\}.check.101[checksetting]

HKCU\software\microsoft\windows\currentversion\action Queries value: center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnosis - diagnosi - diagnosis - diagnosis - diagnosis - diagnosis - diagnosis - d$ scheduled/operational[type]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisscheduled/operational[enabled]

Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosi-diagnosi-diagno-diagnosi-diagno-di$ scheduled/operational[filemax]

Oueries value:

scheduled/operational[filecounter]

 $HKLM \ software \ microsoft \ windows \ -current version \ winevt \ channels \ microsoft -windows - diagnosis - diagnosi - diagnosis - diagnosis - diagnosis - diagnosis - diagnosis - d$ scheduled/operational[buffersize]

 $HKLM \ software \ microsoft \ windows \ -current version \ winevt \ channels \ microsoft -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis \ -diagn$ scheduled/operational[minbuffers]

Oueries value:

 $\label{thm:local-continuous} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft| windows \verb|\currentversion| winevt \verb|\channels| microsoft-windows - diagnosis-microsoft| windows - diagnosis-microsoft| windo$ scheduled/operational[maxbuffers]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnosis - diagnosi - diagnosis - diagnosis - diagnosis - diagnosis - diagnosis - d$ scheduled/operational[latency]

scheduled/operational[clocktype]

 $HKLM \ software \ microsoft \ windows \ -current version \ winevt \ channels \ microsoft -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis \ -diagn$ scheduled/operational[sidtype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisscheduled/operational[level]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisscheduled/operational[controlguid]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ -current version \ winevt \ channels \ microsoft -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis -windows \ -diagnosis \ -diagn$ scheduled/operational[maxsize]

Queries value:

scheduled/operational[maxsizeupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisscheduled/operational[retention]

Oueries value:

scheduled/operational[autobackuplogfiles]

Queries value:

scheduled/operational[file]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisscheduled/operational[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisscheduled/operational[isolation]

Oueries value:

scheduled/operational[owningpublisher]

Queries value:

scheduled/operational[channelaccess]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action$ center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100[checksetting]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ taskscheduler/maintenance[type]

Oueries value:

taskscheduler/maintenance[enabled]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ taskscheduler/maintenance[filemax]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ taskscheduler/maintenance[filecounter]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance[buffersize]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance[minbuffers]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ taskscheduler/maintenance[maxbuffers]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ taskscheduler/maintenance[latency]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ taskscheduler/maintenance[clocktype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance[sidtype]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ taskscheduler/maintenance[level]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ taskscheduler/maintenance[controlguid]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ taskscheduler/maintenance[maxsize]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ taskscheduler/maintenance[maxsizeupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance[retention]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance[autobackuplogfiles]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ taskscheduler/maintenance[file]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ taskscheduler/maintenance[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance[isolation]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ taskscheduler/maintenance[owningpublisher]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ 

taskscheduler/maintenance[channelaccess] Queries value:

HKCU\software\microsoft\windows\currentversion\action center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017\}.check.800[checksetting]

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

 $center \verb|\providers| eventlog \verb|\final 134ea 407-755d-4a93-b8a6-f290cd 155023 \} [lastknown state]$ Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[type]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[enabled]

Queries value:

 $HKLM \ software \ microsoft\ windows \ current version \ winevt\ channels\ microsoft-windows-homegroup \ microsoft\ windows-homegroup \ microsoft\ window$ control panel/operational[filemax]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[filecounter]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[buffersize]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[minbuffers] Queries value:

control panel/operational[maxbuffers]

Queries value:

control panel/operational[latency]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[clocktype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[sidtype]

Oueries value:

 $HKLM \ software \ microsoft\ windows \ current version \ winevt\ channels\ microsoft-windows-homegroup \ microsoft\ windows-homegroup \ microsoft\ window$ control panel/operational[level]

control panel/operational[controlguid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[maxsize]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[maxsizeupper]

Queries value:

control panel/operational[retention]

Queries value:

control panel/operational[autobackuplogfiles]

Queries value:

 $HKLM \ software \ \verb|microsoft| windows \ \verb|currentversion| winevt| \ channels \ \verb|microsoft| - windows \ - homegroup \ \ |$ control panel/operational[file]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational[filterid]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup | leading to the state of the state of$ control panel/operational[isolation]

Oueries value:

control panel/operational[owningpublisher]

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup
control panel/operational[channelaccess]

Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{134ea407-755d-4a93-b8a6-f290cd155023\}.check.8001[checksetting] Oueries value: HKCU\software\microsoft\windows\currentversion\action

center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}[lastknownstate]

Queries value:

Oueries value:

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - security - spp-ux-notifications/actioncenter [filemax]$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - security - spp-ux-notifications/actioncenter [filecounter]$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} winevosoft-windows-security-spp-ux-notifications/actioncenter [buffersize]$ 

Oueries value:

Oueries value

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - security - spp-ux-notifications \ / action center \ [maxbuffers]$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \la$ 

Queries value:

 $\label{thm:hklm} HKLM \software \microsoft-windows-security-spp-ux-notifications/actioncenter[clocktype]$ 

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} winevosoft-windows-security-spp-ux-notifications/actioncenter \cite{thm:hklm} software \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hkllm} hkll \label{lem:hkllm} winevt \label{lem:hkllm} hkll \label{lem:hkkllm} hkll \label{lkkllm} hkll \label{lkkllm} hkll \label{lkkllm} hkll \label{lkkllm} hkll \l$ 

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \la$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - security - spp-ux-notifications/actioncenter \control guid \label{lem:hklm}$ 

Oueries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\mathbb{N}$ icrosoft-windows-security-spp-ux-notifications/actioncenter[maxsizeupper]} \\$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \la$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} wincrosoft-windows-security-spp-ux-notifications/actioncenter [autobackuplogfiles]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - security - spp-ux-notifications/actioncenter [file]$ 

Queries value:

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-security-spp-ux-notifications/actioncenter \cite{thm:loss} is a constant of the control of the control$ 

Queries value

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hkklm} hkll \label{lkklm} hkll \lab$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-ux-notifications/actioncenter[channelaccess]

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

center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100[checksetting]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \sincos of twindows \current version \winevt \channels \sincos of t-windows-file history-core/whc[type]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-file history-core/whc[enabled]$ 

Queries value:

 $\label{lem:hklmsoftware} $$HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-filehistory-core/whc[filemax]$ 

Oueries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-file history-core/whc[filecounter]$ 

Queries value:

Oueries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistorycore/whc[latency]

Queries value:

Oueries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-file \ history-core/\label{thm:local-prop} whc[sidtype]$ 

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-file \ history-core/\label{lem:hklmsoftware} who \cite{the lem of the lem of t$ 

Queries value:

 $\label{lem:hklmsoftware} $$HKLM\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[controlguid]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} cosoft-windows-file history-core/whc[maxsize]$ 

Queries value:

Queries value:

Queries value:

 $HKLM\$  software \microsoft \windows \current version \winevt \channels \microsoft - windows - file history-core/whc[autobackuplogfiles]

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} Consoft-windows-filehistory-core/whc[file]$ 

Oueries value:

 $\label{lem:hammels} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-file \$ 

Queries value:

 $\label{lem:hammels} HKLM \software \microsoft-windows-file history-core/whc[isolation]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistorycore/whc[owningpublisher]

Queries value:

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

 $center \verb|\checks|{b447b4db-7780-11e0-ada3-18a90531a85a}. check. 100[checksetting]|$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[type]
Oueries value:

ntfs/whc[enabled]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[filemax]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-

ntfs/whc[filecounter]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hkklm} Windows \label{lem:hkk$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lkm} \label{lk$ 

Queries value

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Which \label{lem:hklm} windows \label{lem:hklm} with \label{lem:hklm} Which \label{lem:hkklm} Which \label{lem:hkklm}$ 

Queries value:

 $\label{thm:local-prop} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows-ntfs/whc[latency]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} Who \label{lem:hklm} [clock type]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hkklm} Windows \label{lem:hkk$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[level] Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} Windows \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lklm} \label{lklm} \label{lklm} \label{lklm} \label{lkm} \label{lklm} \label{lklm} \label{lklm} \label{lklm} \label{lkm} \label{lklm} \l$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} windows \label{lem:hklm} consoft-windows \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \labell} \label{lklm} \label{lklm} \labell} \label$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-ntfs/whc[maxsizeupper]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} hkll \label{lem:hklm} Who \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \labell} \label{lklm} \label{lkl$ 

Oueries value

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[file]
Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - ntfs/whc[filterid]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[isolation]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[owningpublisher]

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Windows \label{lem:hklm} \label{lklm} \label{lk$ 

Queries value:  $HKCU \ software \ microsoft \ windows \ current version \ action center \ checks \ 3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482 \ . check. \ 100 \ [checksetting]$  Queries value:  $HKCU \ software \ microsoft \ windows \ current version \ action center \ providers \ eventlog \ 2374911b-b114-42fe-900d-54f95fee92e5 \ [lastknown state] \ Oueries \ value:$ 

 $\label{thm:hklm:software} HKLM \software \sicrosoft-windows-shell-connected accounts tate/action center [type]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \ensuremath{\texttt{Microsoft-windows-shell-connected accounts}} tate/action center [enabled]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \ensuremath{\mbox{\mbox{$M$}}} icrosoft-windows-shell-connected accounts tate/action center [file counter]$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} With a microsoft-windows-shell-connected accounts tate/action center [buffer size]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[minbuffers]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} which soft-windows-shell-connected accounts tate/action center [maxbuffers]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \ensuremath{\texttt{Microsoft-windows-shell-connected accounts}} tate/action center \[latency]$ 

Queries value:

 $\label{thm:hklm} HKLM \software \microsoft-windows-current version \winevt \channels \microsoft-windows-shell-connected accounts tate/action center \clock type]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \mbox{$\mbox{$\mathbb{N}$ icrosoft-windows-shell-connected}$} accounts tate/action center [sidtype]$ 

Queries value

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \lab$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \ensuremath{\mbox{\mbox{$M$}}} icrosoft-windows-shell-connected accounts tate/action center [control guid]$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-shell-connected accounts tate/action center \mbox{$[maxsize]$} \\$ 

Queries value:

 $\label{thm:local_hammels_microsoft_windows_shell-connected accounts tate/action center[maxsize upper] } \\$ 

Queries value:

 $\label{thm:hammelsmicrosoft-windows-shell-connected accounts tate/action center [retention]} HKLM\software \mbox{\connected accounts tate/action center [retention]}$ 

Queries value:

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-shell-connected accounts tate/action center [filterid]$ 

Queries value

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} which annels \mbox{\currentversion} winevt \channels \mbox{\currentversion} winevt \channels \mbox{\currentversion} \label{lem:hklm} which is a simple of the lemma of the l$ 

Queries value:

 $\label{thm:local_hammels} HKLM \software \end{time} icrosoft-windows-shell-connected accounts tate/action center [owning publisher]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shell-connectedaccountstate/actioncenter[channelaccess]

Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100[checksetting]

Queries value: HKLM\software\microsoft\w

 $\label{thm:local_hammon_hammon} HKLM \software \microsoft-windows-userpnp/actioncenter[type]$ 

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/actioncenter[enabled]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ userpnp/actioncenter[filemax]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[filecounter]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[buffersize]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ userpnp/actioncenter[minbuffers]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/actioncenter[maxbuffers]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[latency]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ userpnp/actioncenter[clocktype]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/actioncenter[sidtype]

userpnp/actioncenter[level]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/actioncenter[controlguid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[maxsize]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-displayer-based and the property of th$ userpnp/actioncenter[maxsizeupper]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/actioncenter[retention]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/actioncenter[autobackuplogfiles]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ userpnp/actioncenter[file]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/actioncenter[filterid]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/actioncenter[isolation] Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the large that the software \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\color="1" the large that the la$ userpnp/actioncenter[owningpublisher]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[channelaccess]

Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{96f4a050-7e31-453c-88be-9634f4e02139\}.check.8010[checksetting]

Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}[lastknownstate]

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-storage spaces-like \ microsoft-windows \ microsof$ managementagent/whc[type]

Queries value:

managementagent/whc[enabled]

Queries value:

 $HKLM \ software \ microsoft\ windows \ current version \ winevt \ channels \ microsoft\ -windows\ -storage spaces-like \ microsoft\ -windows\ -storage \ -windows\ -storage \ -windows\ -storage \ -windows\ -storage \ -windows\ -windows$ managementagent/whc[filemax]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constant \ channels \ -storage \ -s$ managementagent/whc[filecounter]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constant \ channels \ -storage \ -s$ managementagent/whc[buffersize]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - storage spaces - windows - windows$ managementagent/whc[minbuffers]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc[maxbuffers]

Queries value:

managementagent/whc[latency]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -storage spaces - the software \ -windows \ -window$ managementagent/whc[clocktype]

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc[sidtype]

Oueries value

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc[level]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc[controlguid]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} winevs \lab$ 

Oueries value

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} winevs \lab$ 

Oueries value

 $\label{thm:local_hammels} HKLM \software \mbox{\sc} windows \sc urrent version \mbox{\sc winevt\channels\mbox{\sc microsoft-windows-storages} paces-management \sc windows \$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Wincosoft-windows-storage spaces-management \label{lem:hklm} who \cite{lem:hklm} and \cite{lem:hklm} who \cite{lem:hklm} extracted \cite{lem:hklm} who \cite{lem:hklm} extracted \cite{lem:hklm} who \cite{lem:hklm} extracted \cite{lem:hklm$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Wincosoft-windows-storage spaces-management \label{lem:hklm} when \label{lem:hklm} Figure \label{lem:hklm} Alter \label{lem:hklm} Whice \label{lem:hkklm} Whice \label{lem$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\sc} windows \sc urrent version \mbox{\sc winevt\channels\mbox{\sc windows-storage} paces-management \sc windows \$ 

Queries value:

 $\label{lem:hklm} HKLM \noinder \noind$ 

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} wincrosoft-windows-storage spaces-management \label{lem:hklm} wincrosoft-wincrosoft-windows-storage spaces-management \label{lem:hklm} wincrosoft-wincrosoft-windows-storage spaces-management \label{lem:hklm} wincrosoft-windows-storage spaces-management \label{lem:hklm} wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincrosoft-wincr$ 

Oueries value:

 $\label{lem:hklm} HKLM \software \mbox{\sc} windows \sc} winevt \channels \mbox{\sc} windows \sc} storage spaces-management \sc} whe \cline{lem:hklm} crosoft-windows \sc} an age mentagent \sc/\sc{hklm} crosoft-windows \sc} an age mentagent \sc} whe \cline{lem:hklm} crosoft-windows \sc} an age mentagent \sc} an age \sc{hklm} crosoft-windows \sc} an age \sc} an age \sc{hklm} crosoft-windows \sc} an age \sc} an a$ 

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

 $center \verb|\checks|{aa4c798d-d91b-4b07-a013-787f5803d6fc}|. check. 100[checksetting]|$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{96f4a050-7e31-453c-88be-9634f4e02139\}[]$ 

Queries value:

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \microsoft \windows \current version \winevt \publishers \end{4.5} \{96f4a050-7e31-453c-88be-9634f4e02139\} \cite{Absolute of the control of the co$ 

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{$1-453c-88be-9634f4e02139} [parameter filename]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{96f4a050-7e31-453c-88be-9634f4e02139\} \ [helplink]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{96f4a050-7e31-453c-88be-9634f4e02139\} \ [enabled]$ 

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{$$ Windows \circ \mbox{$$ urrentversion \mbox{$$ winevt <page-header> $$ 96f4a050-7e31-453c-88be-9634f4e02139 \category count]} $$$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} which software \label{lem:hklm} with the highest lemma software \label{lem:hklm} which is a simple software \label{lem:hklm} which is a simple software \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hkllm} hkll \label{lem:hkllm} hkll \label{lem:hkllm} hkll \label{lem:hkkllm} hkll \label{lem:hkklllm} hkll \label{lem:hkklllm} hkll \label{lem:hkkllm} hkll \label{lem:hkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkkllm} hkll \label{lkklllm} hkll \labell{lkklllm} hkll \labell{lkklllm} hkll \labell{lkklllm} hkll \labell{lkklllm} hkll \labell{lkklllm} hkll \labell{lkkllm} hkll \labell{lkklllm} hkll \labell{lkklllm} hkll \labell{lkkll$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-userpnp/scheduler operations \cite{thm:local-prop} \end{substitute} and \cite{thm:local-prop} \mbox{\cite{thm:local-prop}} \mbox{\$ 

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} Windows \label{lem:hklm} winevt \label{lem:hklm} Windows \label{lem:hklm} winevt \$ 

Queries value:

 $\label{thm:loss-twindows} HKLM \software \mbox{\sc} windows \screen \scalebox{\sc} winevt \channels \mbox{\sc} windows \screen \scalebox{\sc} windows \screen \scalebox{\sc} winevt \channels \mbox{\sc} windows \screen \scalebox{\sc} windows \scalebox{$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hklm \label{lem:hklm} hklm \label{lem:hklm} hklm \label{lem:hklm} hklm \label{lem:hklm} hklm \label{lem:hklm} hklm \label{lem:hklm} winevt \label{lem:hklm} hklm \label{lklm} hklm$ 

Queries value:

 $HKLM \label{lem:hklm} In the constant of the$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/scheduleroperations[maxbuffers]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/scheduleroperations[latency]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \lab$ 

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/scheduleroperations[sidtype]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the property of the prope$ userpnp/scheduleroperations[level]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/scheduleroperations[keywordslower]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/scheduleroperations[keywordsupper]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the property of the prope$ userpnp/scheduleroperations[controlguid]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/scheduleroperations[maxsize]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/scheduleroperations[maxsizeupper]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ userpnp/scheduleroperations[retention]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/scheduleroperations [autobackuplog files]

userpnp/scheduleroperations[file]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/scheduleroperations[filterid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/scheduleroperations[isolation]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ userpnp/scheduleroperations[owningpublisher]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/scheduleroperations[channelaccess]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[type]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[enabled]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/performance[filemax]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/performance[filecounter] Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the large that the software \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\color="1" the large that the la$ userpnp/performance[buffersize]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[minbuffers] Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[maxbuffers]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ userpnp/performance[latency]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[clocktype]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[sidtype]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/performance[level]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/performance[keywordslower]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/performance[keywordsupper]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[controlguid]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ userpnp/performance[maxsize]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/performance[maxsizeupper]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/performance[retention]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the property of the prope$ userpnp/performance[autobackuplogfiles]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[file]

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$}$-windows-current} $$ in \mbox{$\mbox{$\mbox{$w$inevt$}$-windows-current} $$ in \mbox{$\mbox{$\mbox{$\mbox{$w$inevt$}$}$-windows-current} $$ in \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$w$inevt$}$}$}$} in \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$w$inevt$}$}$}$}$} in \mbox{$\mbo$ userpnp/performance[filterid]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the property of the prope$ userpnp/performance[isolation]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/performance[owningpublisher]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/performance[channelaccess]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ userpnp/devicemetadata/debug[type]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/devicemetadata/debug[enabled]

userpnp/devicemetadata/debug[filemax]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[filecounter]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/devicemetadata/debug[buffersize]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-displayer-based and the property of th$ userpnp/devicemetadata/debug[minbuffers]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/devicemetadata/debug[maxbuffers]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/devicemetadata/debug[latency]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/devicemetadata/debug[clocktype]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[sidtype]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[level] Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the state of the stat$ 

userpnp/devicemetadata/debug[keywordslower] Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/devicemetadata/debug[keywordsupper] Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-displayer-based and the property of th$ userpnp/devicemetadata/debug[controlguid]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ userpnp/devicemetadata/debug[maxsize]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[maxsizeupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/devicemetadata/debug[retention]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[autobackuplogfiles]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[file]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ userpnp/devicemetadata/debug[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/devicemetadata/debug[isolation]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - windows - windows \cdot winevt \setminus channels \setminus microsoft - windows - windows \cdot wi$ userpnp/devicemetadata/debug[owningpublisher]

Queries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ userpnp/devicemetadata/debug[channelaccess]

Sets/Creates value

```
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
  Sets/Creates value:
                                      HKLM\system\currentcontrolset\services\nativewifip[ndismajorversion]
                                      HKLM\system\currentcontrolset\services\nativewifip[ndisminorversion]
  Sets/Creates value:
                                      HKLM\system\currentcontrolset\services\nativewifip[drivermajorversion]
  Sets/Creates value:
  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]
  Sets/Creates value:
                                      HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dhcpnameserver]
  Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
  Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpsubnetmaskopt]
  Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdefaultgateway]
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34[]
  Sets/Creates value:
                                      HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Value changes:
context logger[status]
  Value changes:
                                      HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet[{b5105d63-74c6-4dc1-87b7-55779daa70e9}]
                                      HKU\s-1-5-21-1923240461-1905901954-2556564120-
  Value changes:
1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility
assistant\store[c:\windows\temp\toggleservice32.exe]
  Value changes:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
  Value changes:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\fb5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpinterfaceoptions]
  Value changes:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ user as sist \ \{cebff5cd-ace2-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f4f-9178-4f78-4f78-4f78-4f78-4f78-
9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
  Value changes:
9926f41749ea}\count[hrzr_pgyfrffvba]
                                      HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[servicesessionid]
  Value changes:
                                      HKLM\software\microsoft\security center[cval]
  Value changes:
                                      HKLM\software\microsoft\security center\svc[antivirusoverride]
  Value changes:
                                      HKLM\software\microsoft\security center\svc[antispywareoverride]
                                      HKLM\software\microsoft\security center\svc[firewalloverride]
  Value changes:
  Value changes:
                                      HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[licstatusarray]
  Value changes:
                                      HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[actionlist]
  Value changes:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
  Value changes:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.103[checksetting]
                                      \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\action}} \\
  Value changes:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100[checksetting]
                                      HKCU\software\microsoft\windows\currentversion\action
  Value changes:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.102[checksetting]
                                      HKCU\software\microsoft\windows\currentversion\action
  Value changes:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100[checksetting]
                                      HKCU\software\microsoft\windows\currentversion\action
  Value changes:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting]
  Value changes:
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc\}.check.0[checksetting]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
  Value changes:
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1\}.check.0[checksetting]
```