Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 5, Task ID: 14

Task ID: 14 Risk Level:

Date Processed: 2016-04-07 08:21:31 (UTC)

Processing Time: 61.18 seconds

IntelliVM Virtual Environment:

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

Sample ID: Type: basic Owner: admin

ToggleService32.exe Label: Date Added: 2016-04-07 08:21:31 (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

Injects thread into Windows process

2 Resolves local hostname 6 PE: File has TLS callbacks

3 Writes to a log file [Info]

4 Terminates process under Windows subfolder

4 Reads process memory

4 Connects to local IP

5 Installs service

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]

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]

C:\Windows\system32\svchost.exe [C:\Windows\system32\svchost.exe -k

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]

C:\Windows\System32\conhost.exe

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

LocalSystemNetworkRestricted]

Reads from process: PID:2356 C:\Windows\SysWOW64\calc.exe
Terminates process: C:\Windows\System32\alg.exe
Terminates process: C:\Windows\System32\UIODetect.exe
Terminates process: C:\Windows\System32\VSSVC.exe

Terminates process: C:\Windows\System32\svchost.exe
Terminates process: C:\Windows\Temp\ToggleService32.exe

Creates remote thread: System

Terminates process:

Creates remote thread: C:\Windows\System32\svchost.exe
Creates remote thread: C:\Windows\explorer.exe
Creates remote thread: C:\Windows\System32\services.exe

Creates remote thread: C:\Windows\System32\services.exe
Creates remote thread: C:\Windows\System32\sppsvc.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\MSDTC_STATS_EVENT

Creates mutex: \BaseNamedObjects\{00358dad-0e96-4bd1-837d-96e6cdd42d3b}_S-1-5-19

Creates mutex: \BaseNamedObjects\WIATRACE_MUTEX

Creates mutex: \BaseNamedObjects\\d3b1bbc7-c020-4056-9ded-7c6f40b5a2fc
Creates mutex: \BaseNamedObjects\\{11517B7C-E79D-4e20-961B-75A811715ADD\}

Creates event: \BaseNamedObjects\RouterPreInitEvent

Creates event: \BaseNamedObjects\AudioSrv_CanAcceptMMCClient
Creates event: \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

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

C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg

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

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

Creates:

Creates:

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

Creates:

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

Creates: C:\Windows\Debug\WIA

Creates: C:\Windows\ServiceProfiles\LocalService

 ${\it C:\Windows\ServiceProfiles\LocalService\AppData\Local}$

 $\label{lem:creates:C:Windows} Creates: C: \windows \scalebox{$\operatorname{C:\windows}$} Creates: C: \windows \scalebox{$\operatorname{C:\windows}$} Creates \scalebox{$\operatorname{C:\wind$

Creates: C:\Windows\SoftwareDistribution

Creates: C:\Windows\System32\spp\store\data.dat.tmp

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC

 $\label{local_microsoftwindows} C: \label{local_microsoftwindows} WER\ERC\statecache.lock and \label{local_microsoftwindows} \label{loca$

Opens: C:\Windows\Prefetch\TOGGLESERVICE32.EXE-2248A864.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

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

 $\begin{tabular}{ll} Opens: & C:\windows\system32\ole32.dl1 \\ Opens: & C:\windows\system32\uxtheme.dl1 \\ \end{tabular}$

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

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

Opens: C:\Windows\System32\en-US\user32.dll.mui
Opens: C:\Windows\system32\uxtheme.dll.Config

Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f

 $\label{lem:controls_659564144ccf1df_6.0.9200.16384_none_418c2a697189c07f\\ \verb|comtrols_659564144ccf1df_6.0.9200.16384_none_418c2a697189c07f\\ \verb|comtrols_6595641446_none_418c2a697189c07f\\ \verb|comtrols_6595641466_none_418c2a697189c07f\\ \verb|comtrols_659666_none_418c2a697189c07f\\ \verb|comtrols_65966_none_418c2a697189c07f\\ \verb|comtrols_6596_none_418c2a697189c07f\\ \verb|com$

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

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

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll

```
Opens:
                          C:\Windows\SysWOW64\cryptbase.dll
 Opens:
                          C:\Windows\SysWOW64\sspicli.dll
 Opens:
                          C:\Windows\SysWOW64\rpcrt4.dll
                          C:\Windows\SysWOW64\advapi32.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\output.txt
                          C:\Windows\Prefetch\ALG.EXE-1D11534C.pf
 Opens:
 Opens:
                          C:\Windows\System32
                          C:\Windows\System32\mswsock.dll
 Opens:
                          C:\Windows\System32\clbcatq.dll
 Opens:
 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:
                          C:\Windows\System32\msdtcprx.dll
 Opens:
 Opens:
                          C:\Windows\System32\msdtclog.dll
 Opens:
                          C:\Windows\System32\mtxclu.dll
 Opens:
                          C:\Windows\System32\winmm.dll
 Opens:
                          C:\Windows\System32\clusapi.dll
 Opens:
                          C:\Windows\System32\bcrypt.dll
                          C:\Windows\System32\xolehlp.dll
 Opens:
 Opens:
                          C:\Windows\System32\dnsapi.dll
 Opens:
                          C:\Windows\System32\ktmw32.dll
 Opens:
                          C:\Windows\System32\resutils.dll
 Opens:
                          C:\Windows\System32\winmmbase.dll
 Opens:
                          C:\Windows\System32\cryptdll.dll
 Opens:
                          C:\Windows\System32\en-US\msdtc.exe.mui
                          C:\Windows\System32\comres.dll
 Opens:
 Opens:
                          C:\Windows\System32\msdtcVSp1res.dll
 Opens:
                          C:\Windows\System32\mtxoci.dll
                          C:\Windows\System32\MsDtc\Trace
 Opens:
 Opens:
                          C:\Windows\System32\sspicli.dll
                          C:\Windows\DtcInstall.log
 Opens:
                          C:\Windows\System32\ntmarta.dll
 Opens:
 Opens:
                          C:\Windows\System32\MsDtc
 Opens:
                          C:\Windows\System32\MsDtc\MSDTC.LOG
 Opens:
                          C:\Windows\System32\en-US\msdtcVSp1res.dll.mui
                          C:\Windows\System32\FirewallAPI.dll
 Opens:
 Opens:
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
AppXDeploymentServer%4Operational.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Opens:
NetworkProfile%4Operational.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
 Opens:
StoreMgr%4Operational.evtx
                          C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Opens:
{\tt DeviceSetupManager\%40perational.evtx}
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Opens:
UserPnp%4DeviceInstall.evtx
 Opens:
                          C:\Windows\Prefetch\UI0DETECT.EXE-A794C8BB.pf
                          C:\Windows\System32\wtsapi32.dll
 Opens:
 Opens:
                          C:\Windows\System32\version.dll
 Opens:
                          C:\Windows\System32\winsta.dll
                          C:\Windows\System32\en-US\ui0detect.exe.mui
 Opens:
 Opens:
                          C:\Windows\System32\adtschema.dll
                          C:\Windows\System32\services.exe
 Opens:
                          C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
 Opens:
 Opens:
                          C:
                         C:\$Extend
 Opens:
 Opens:
                          C:\ProgramData
                          C:\ProgramData\Microsoft
 Opens:
 Opens:
                          C:\ProgramData\Microsoft\Crypto
 Opens:
                          C:\ProgramData\Microsoft\Crypto\RSA
 Opens:
                          C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
                          C:\Windows\Globalization
 Opens:
 Opens:
                          C:\Windows\Globalization\Sorting
 Opens:
                          C:\Windows\ServiceProfiles
 Opens:
                          C:\Windows\ServiceProfiles\LocalService
 Opens:
                          C:\Windows\ServiceProfiles\LocalService\AppData
 Opens:
                          C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
                          {\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft}
 Opens:
 Opens:
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates}
 Opens:
{\tt C:\Windows\Service\Profiles\LocalService\AppData\Roaming\Microsoft\System\Certificates\My}
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates}
                          C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
 Opens:
 Opens:
                          C:\Windows\System32\en-US
 Opens:
                          C:\Windows\System32\ntdll.dll
 Opens:
                          C:\Windows\System32\kernel32.dll
                          C:\Windows\System32\KernelBase.dll
 Opens:
                          C:\Windows\System32\locale.nls
 Opens:
 Opens:
                          C:\Windows\System32\svchost.exe
                          C:\Windows\System32\rpcrt4.dll
 Opens:
 Opens:
                          C:\Windows\System32\pnrpsvc.dll
 Opens:
                          C:\Windows\System32\msvcrt.dll
 Opens:
                          C:\Windows\System32\gpapi.dll
  Opens:
                          C:\Windows\System32\powrprof.dll
                          C:\Windows\System32\profapi.dll
 Opens:
```

```
Opens:
                                     C:\Windows\System32\crypt32.dll
  Opens:
                                     C:\Windows\System32\msasn1.dll
  Opens:
C:\PROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\358129098041A0483A25B784E8E10913_DE228479-9E18-
473A-B3D7-31D4D2573DC2
                                     C:\Windows\System32\en-US\crypt32.dll.mui
  Opens:
  Opens:
                                     C:\Windows\Svstem32\dpapi.dll
  Opens:
                                     C:\Windows\System32\ncrypt.dll
                                     C:\Windows\System32\ntasn1.dll
  Opens:
  Opens:
                                     C:\Windows\System32\QAGENTRT.DLL
                                     C:\Windows\System32\en-US\QAgentRT.dll.mui
  Opens:
  Opens:
                                     C:\Windows\System32\en-US\dnsapi.dll.mui
  Opens:
                                     C:\Windows\System32\fveui.dll
  Opens:
                                     C:\Windows\System32\en-US\fveui.dll.mui
                                     C:\Windows\System32\wuaueng.dll
  Opens:
                                     C:\Windows\System32\en-US\wuaueng.dll.mui
  Opens:
  Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
                                    C:\Windows\System32\advapi32.dll
  Opens:
  Opens:
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:
  Opens:
                                     C:\Windows\System32\nsi.dll
  Opens:
                                     C:\Windows\System32\IPHLPAPI.DLL
  Opens:
                                     C:\Windows\System32\winnsi.dll
  Opens:
                                     C:\Windows\System32\dhcpcsvc6.dll
                                     C:\Windows\System32\dhcpcsvc.dll
  Opens:
                                     C:\Windows\System32\sqmapi.dll
  Opens:
  Opens:
                                     C:\Windows\System32\gdi32.dll
  Opens:
                                     C:\Windows\System32\en-US\svchost.exe.mui
  Opens:
                                     C:\Windows\System32\oleaut32.dll
  Opens:
                                     C:\Windows\System32\ssdpapi.dll
  Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\5fe46d6f4fbbaedee4917a93b3902d78_de228479-9e18-
473a-b3d7-31d4d2573dc2
  Opens:
                                     C:\Windows\System32\p2psvc.dll
                                     C:\Windows\System32\P2PGraph.dll
  Opens:
  Opens:
                                     C:\Windows\System32\esent.dll
                                     C:\Windows\System32\en-US\p2psvc.dll.mui
  Opens:
  Opens:
                                     C:\Windows\System32\authz.dll
  Opens:
                                     C:\Windows\System32\secur32.dll
  Opens:
                                     C:\Windows\System32\slc.dll
  Opens:
473a-b3d7-31d4d2573dc2
  Opens:
C: \windows \Service Profiles \Local Service \App Data \Roaming \Microsoft \System Certificates \My \Certificates \9C99BD1474CEB9C1AB13129747684184429ED3A1 \Roaming \Microsoft \System Certificates \Ny \Certificates \Profiles \Profiles \Profiles \Roaming \Roaming
  Opens:
473a-b3d7-31d4d2573dc2
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\31df4714b46f5e5ff8248d0fafa3b957_de228479-9e18-
473a-b3d7-31d4d2573dc2
  Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\907a2f9ea01e84ee4723362858705197.sst
  Opens:
                                     C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
  Opens:
                                     C:\Windows\Svstem32\spoolsv.exe
                                     C:\Windows\System32\en-US\spoolsv.exe.mui
  Opens:
                                     C:\Windows\System32\drivers\etc\lmhosts
  Opens:
  Opens:
                                     C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
  Opens:
                                     C:\Windows\System32\VSSVC.exe
  Opens:
                                     C:\Windows\System32\vssapi.dll
  Opens:
                                     C:\Windows\System32\vsstrace.dll
                                     C:\Windows\System32\virtdisk.dll
  Opens:
  Opens:
                                     C:\Windows\System32\dsrole.dll
  Opens:
                                     C:\Windows\System32\fltLib.dll
  Opens:
                                     C:\Windows\System32\en-US\VSSVC.exe.mui
  Opens:
                                     C:\Windows\System32\vss_ps.dll
                                     C:\Windows\System32\en-US\vsstrace.dll.mui
  Opens:
                                     C:\Windows\System32\samcli.dll
  Opens:
  Opens:
                                     C:\Windows\System32\netutils.dll
  Opens:
                                     C:\Windows\System32\samlib.dll
  Opens:
                                     C:\Windows\System32\es.dll
  Opens:
                                     C:\Windows\System32\propsys.dll
  Opens:
                                     C:\Windows\System32\catsrvut.dll
                                     C:\Windows\System32\mfcsubs.dll
  Opens:
  Opens:
                                     C:\Windows\System32\sxs.dll
  Opens:
                                     C:\Windows\System32\eventcls.dll
  Opens:
                                     C:\Windows\System32\stdole2.tlb
  Opens:
                                     C:\Windows\System32\msxml3.dll
  Opens:
                                     C:\Windows\System32\shlwapi.dll
                                     C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:
                                     C:\Windows\System32\msxml3r.dll
  Opens:
                                     C:\Windows\System32\setupapi.dll
  Opens:
  Opens:
                                     C:\Windows\System32\cfgmgr32.dll
  Opens:
                                     C:\Windows\System32\devobj.dll
  Opens:
                                     C:\Windows\System32\en-US\setupapi.dll.mui
                                     C:\Windows\System32\wintrust.dll
```

Opens:

```
Opens:
                                                                                                                                                 C:\Windows\System32\audiosrv.dll
           Opens:
                                                                                                                                                 C:\Windows\System32\hid.dll
           Opens:
                                                                                                                                                 C:\Windows\System32\avrt.dll
                                                                                                                                                 C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
           Opens:
           Opens:
                                                                                                                                                 C:\Windows\System32\wersvc.dll
                                                                                                                                                 C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
          Opens:
           Opens:
                                                                                                                                                 C:\Windows\debug
                                                                                                                                                 C:\Windows\debug\WIA
          Opens:
                                                                                                                                                 C:\Windows\System32\wiaservc.dll
           Opens:
          Opens:
                                                                                                                                                 C:\Windows\System32\wiatrace.dll
           Opens:
                                                                                                                                                 C:\Windows\System32\msv1_0.dll
          Opens:
                                                                                                                                                 C:\Windows\System32\sti.dll
           Opens:
                                                                                                                                                 C:\Windows\debug\WIA\wiatrace.log
           Opens:
                                                                                                                                                 C:\Windows\System32\Drivers\nwifi.sys
                                                                                                                                                 C:\Windows\apppatch\drvmain.sdb
           Opens:
                                                                                                                                                 C:\Windows\System32\Drivers\ndisuio.sys
           Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
           Opens:
           Opens:
                                                                                                                                                 C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
                                                                                                                                                 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:
 US~6.2.9200.16384.cat
           Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Hyper-V-ClientEdition-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^-6.2.9200.16384. \\ categorian \\ 
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \texttt{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}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
          Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \text{Microsoft-Hyper-V-Management-PowerShell-Package-net-} \\ 31bf3856ad364e35 \\ \text{-amd} \\ 64\text{-en-package-net-} \\ \text{-amd} \\ \text{-amd}
 US~6.2.9200.16384.cat
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
  00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-
 net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package~31bf3856ad364e35~amd64~en-
 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
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
          Opens
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \text{Microsoft-Hyper-V-Package-termsrv-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \\ \text{Constant of the proposed of the p
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE\} \\ \texttt{Microsoft-Hyper-V-Package-termsrv-31bf3856ad364e35-amd64--6.2.9200.16384.cat} \\ \\ \texttt{Constant} 
          Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE \} \\ Microsoft-Hyper-V-Server-Drivers-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Drivers-Package \\ \sim amd64 \\ \sim amd64
US~6.2.9200.16384.cat
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE \} \\ \text{Microsoft-Hyper-V-Server-Drivers-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat} \\ \text{Constant of the properties o
          Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Media-Foundation-Package ~31bf3856ad364e35 ~amd64~en-US~6.2.9200.16384.cat
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Media-Foundation-Package ~31bf3856ad364e35 \\ \\ ~amd64 \\ \\ ~6.2.9200.16384.cat \\ \\ ~6.2.9200.cat \\ \\ ~6.2.9200.16384.cat \\ \\ ~6.2.9200.16384.cat \\ \\ ~6.2.9200.cat \\ \\ ~6.2
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
  00C04FC295EE}\Microsoft-Virtualization-Client-Interop-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE\} \\ \ Microsoft-Windows-Anytime-Upgrade-Package-31bf3856ad364e35-amd64-en-defined by the control of the control 
 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:
  00C04FC295EE\}\\ Microsoft-Windows-Anytime-Upgrade-Results-Package-31bf3856ad364e35-amd64-en-Bound Control of the Control of t
 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-
          Opens:
 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:
 {\tt 00C04FC295EE} \verb+\Microsoft-Windows-ApisetNamespace-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-AvCore-Av
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
           Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
           Opens:
                                                                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-Mincore-Package ~ 31bf3856ad364e35 ~ amd 64 ~ en-package ~ 31bf3866ad364e35 ~ amd 64 ~ en-package ~ 
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\} \\ Microsoft-Windows-ApisetNamespace-Minio-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^en-Minio-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^am-Minio-Package \\ ^31bf3856ad364e35 \\ ^am-Minio-Package \\ ^31bf3864ad364e35 \\ ^am-Minio-Package \\ ^31bf3864ad364e35 \\ ^am-Minio-Package \\ ^31bf3864ad36464 \\ ^am-Minio-Package \\ ^31bf3864ad364 \\ ^am-Minio-Package \\ ^31
US~6.2.9200.16384.cat
    Opens:
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-
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:
US~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\}\\ Microsoft-Windows-ApisetNamespace-WOW64-Minio-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-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
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-
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 ~ endown a constraint of the constraint
US~6.2.9200.16384.cat
        Opens:
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-W0W64-Windows-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-Package~31bf3856ad364e35~amd64~en-M10008-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~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~amd66e
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
        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-Backup-Package \\ ^{3}1bf3856ad364e35 \\ ^{a}md64 \\ ^{a}6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
00C04FC295EE}\Microsoft-Windows-Basic-Http-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
         Opens:
                                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-Basic-Http-Package-31bf3856ad364e35-amd64-en-100c04FC295EE \verb+\Microsoft-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows-Basic-Windows
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-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\} \\ Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bootEnvironment-Dvd-Package-minkernel \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bootEnvironment-Dvd-Package-minkernel \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bootEnvironment-Dvd-Package-minkernel \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bootEnvironment-Dvd-Package-minkernel \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bootEnvironment-Dvd-Package-minkernel \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-bootEnvironment-Dvd-Package-minkernel \\ \sim en-bootEnvironment-Dvd-Package-min
US~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package~31bf3856ad364e35~amd64~en-
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
        Opens:
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Branding-Professional-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-fine \\ \sim amd64 \\ \sim en-fine \\ \sim amd64 \\ \sim a
US~6.2.9200.16384.cat
        Opens:
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Branding-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Branding-Professional WMC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-fine the control of the contro
US~6.2.9200.16384.cat
        Onens:
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Business Scanning-Feature-Package-admin~31bf3856ad364e35~amd64~en-defendant for the control of the contro
US~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                              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:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-BusinessScanning-Feature-Points} \\
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Windows-Client-Drivers-Package-drivers-31bf3856ad364e35\\ \\ -amd64\\ -en-drivers-21bf3856ad364e35\\ \\ -amd64\\ \\
US~6.2.9200.16384.cat
        Opens:
                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                              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-
00C04FC295EE\} \\ Microsoft-Windows-Client-Drivers-Package-multimedia ~31bf3856ad364e35 ~amd64 ~en-drivers-Package-multimedia ~31bf3856ad364e35 ~amd64 ~amd6
```

```
US~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                              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:
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-
US~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
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\} \\ \mbox{Microsoft-Windows-Client-Drivers-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim ended
US~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Client-Features-Package-avcore} \\ \mbox{31bf3856ad364e35-amd64-en-package-avcore} \\ \mbox{21bf3856ad364e35-amd64-en-package-avcore} \\ \mbox{22bf3856ad364e35-amd64-en-package-avcore} \\ \mbox{22bf3866ad364e35-amd64-en-package-avcore} \\ \mbox{22bf3866ad364e35-amd64-en-package-avcore} \\ \mbox{22bf3866ad364e35-amd64-en-package-avcore} \\ \mbox{22bf3866ad364-en-package-avcore} \\ \mbox{22bf3866ad364-en-package-avcor
US~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-Client-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows
US~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                              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~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~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~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~am
US~6.2.9200.16384.cat
      Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
 inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
 inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                              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-
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
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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-
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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 \sim 31bf3856ad364e35-amd64 \sim en-constraints of the constraints 
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan-31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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
      Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package-terms rv~31bf3856ad364e35~amd64~en-defined by the second statement of the second stateme
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
      Opens:
                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-leaved} \\ \mbox{Microsoft-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windows-Client-Windo
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: \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-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
      Opens:
                                                                                             C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
 00C04FC295EE}\Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
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-ended \\ ~31bf3856ad364-amd64-ended \\ ~31bf3856ad364-amd64-ended \\ ~31bf3856ad364-amd64-ended \\ ~31bf3856ad364-amd64-ended \\ ~31bf3866ad364-amd64-ended \\ ~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-a
US~6.2.9200.16384.cat
      Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ Microsoft-Windows-COM-MSMQ-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~en-
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-
      Opens:
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-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-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-DriverClasses-Common-Dr
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~en-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~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~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5~amd64ad5
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-
         Opens:
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Windows-Common-Drivers-Package-drivers-31bf3856ad364e35-amd64-ended from the common of the common of
US~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-Common-Drivers-Package-minio~31bf3856ad364e35~amd64~enderserved by the common of the commo
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 \} \verb|\microsoft-Windows-Common-Drivers-Package-minkernel-31bf3856ad364e35-amd64-en-defined by the common-Drivers-Package-minkernel-31bf3856ad364e35-amd64-en-defined by the common-Drivers-Package-minkernel-31bf3856ad364-amd64-en-defined by the common-Drivers-Package-minkernel-31bf3856ad364-amd64-en-defined by the common-Drivers-Package-minkernel-31bf3856ad36-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-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\} \\ \mbox{Microsoft-Windows-Common-Drivers-Package-net-$31bf3856ad364e35-$amd64-en-lem-of-section of the common-of-section of the co
US~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                       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-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-31bf3856ad364-amd64-en-drivers-package-vm-31bf3856ad364-en-drivers-package-vm-31bf3856ad364-en-drivers-package-vm-31bf3856ad364-en-drivers-package-vm-31bf3856ad364-en-drivers-package-vm-31bf3856ad364-en-drivers-package-vm-31bf3864-en-drivers-package-vm-31bf3864-en-drivers-package-vm-31bf3864-en-drivers-package-vm-
US~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
vm~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
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-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-Package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3856ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-31bf3866ad364e35-amd64-en-drivers-package-net-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-amd64-amd64-amd64-amd64-amd64-amd64-amd64-am
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
                                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
US~6.2.9200.16384.cat
        Onens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-CommonFoundation-LanguagePack-Package \\ \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:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-CoreSystem-Com-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3866ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3866ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3866ad364 \\ \sim en-Package \\ \sim 
US~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-CoreSystem-Com-Package-31bf3856ad364e35-amd64$$\sim$6.2.9200.16384.cat and the contract of the contract
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
OOCO4FC295EE}\Microsoft-Windows-CoreSystem-Mincore-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-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-CoreSystem-Net-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-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-RemoteFS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                         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-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3856ad364e35-amd64-en-Base-Package~31bf3866ad364e35-amd64-en-Base-Package~31bf3866ad364e35-amd64-en-Base-Package~31bf3866ad366-amd64-en-Base-Package~31bf3866ad366-amd64-en-Base-Package~31bf3866ad366-amd64-en-Base-Package~31bf3866ad366-amd64-en-Base-Package~31bf3866ad366-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-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
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                         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
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\}\\ Microsoft-Windows-CoreSystem-WOW64-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~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~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
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-CoreSystem-WOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-backage \\ \sim 100004 \\
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
    Opens:
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
```

```
Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    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: \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-DirectoryServices-ADAM-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \backslash {\tt microsoft-windows-directory} services-adam-snapins-package-constraints and {\tt output} services are services and {\tt output} services and {\tt output} services are services are services are services are services are se
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ \ Microsoft-Windows-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Disk-Diagnosis-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Disk-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagnosis-Diagno
US~6.2.9200.16384.cat
     Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-Editions-Professional WMC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-100c04FC295EE \\ \sim 100c04FC295EE \\ \sim 100c04FC2
US~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-Editions-ProfessionalWMC-Professional} \\
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\}\\ Microsoft-Windows-Foundation-Package ~31bf3856ad364e35-amd64-~6.2.9200.16384.cat
                                                                                   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-
     Opens:
{\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~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00 Co4FC295EE \} \\ Microsoft-Windows-Group Policy-Client Tools-Package-admin~31bf3856ad364e35~amd64~en-defendable for the control of the con
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-
00C04FC295EE\} \\ Microsoft-Windows-GroupPolicy-ClientTools-Package-base~31bf3856ad364e35~amd64~en-base \\ And the first of the first of
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
     Opens:
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
```

```
Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  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-
     Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \texttt{Microsoft-Windows-GroupPolicy-ClientTools-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-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e35-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-en-minio-31bf3866ad364e36-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-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-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-
     Opens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
{\tt OOCO4FC295EE} \verb+\Microsoft-Windows-GroupPolicy-ClientTools-Package-Fine Policy-ClientTools-Package-Fine Policy-ClientFine Policy-Client
multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  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-
{\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-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-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
printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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-Fourier} \\
 termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00 \\ Co4FC295EE \} \\ Microsoft-Windows-Group \\ Policy-Client \\ Tools-Package-31bf3856ad364e35-amd64-ended \\ Policy-Client \\ Policy-Cl
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-HandwritingRecognizer-Package-31bf3856ad364e35-amd64-en-defined by the control of the co
US~6.2.9200.16384.cat
      Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  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-Help-ClientUA-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
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-
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:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-Identity-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
                                                                                                                                              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-
          Opens:
  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:
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
           Opens:
  00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE\}\\ Microsoft-Windows-IIS-WebServer-Package ~31bf3856ad364e35 ~amd64 ~~ 6.2.9200.16384. cat a constant of the con
                                                                                                                                              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-ImageBasedSetup-IE-Package-
 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~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~31bf3856ad364e35~amd64~enduser~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~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
          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-
 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-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-31bf3856ad364-amd64-en-Package-windows-31bf3856ad364-amd64-en-Package-windows-31bf3856ad364-amd64-en-Package-windows-31bf3856ad364-amd64-en-Package-windows-31bf3856ad364-amd64-en-Package-windows-31bf3856ad364-amd64-en-Package-windows-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-amd
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-ImageBasedSetup-IE-Package-
 windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~en-
 US~10.0.9200.16384.cat
          Opens:
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-
 Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 00C04FC295EE\} \verb+\Microsoft-Windows-InternetExplorer-Package-shell-31bf3856ad364e35-amd64-en-defined by the control of the co
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
 shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
 ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE \} \\ \label{lem:condition} Internet Explorer-Package \sim 31bf3856ad364e35 \sim amd 64 \sim end of the condition of the 
 US~10.0.9200.16384.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-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
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
  00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
 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 \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage-avcore \\ \sim 11bf3856ad364e35 \\ \sim en-brackage-avcore \\ \sim en-b
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
 avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-Media-Format-Package-windows-31bf3856ad364e35-amd64-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-endown-2006-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: \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-Media-Format-Package ~31bf3856ad364e35 ~amd 64 ~~ 6.2.9200.16384. cat a constant of the co
          Opens:
                                                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-Media-Streaming-Package-31bf3856ad364e35-amd64-en-defined and the control of the con
 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
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-avcore~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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-
 00C04FC295EE\} \\ Microsoft-Windows-MediaCenter-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim 6.2.9200.16384. \\ categorian \\
         Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
         Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-MediaPlayer-Package-avcore} \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\ \sim en-beta = 100c04FC295EE \\ \sim amd 64 \\
 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} \backslash {\tt Microsoft-Windows-MediaPlayer-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-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
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  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
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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
         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-MediaPlayer-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
         Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE\} \\ Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-defendable for the control of the control o
US~6.2.9200.16384.cat
                                                                                                                                          {\tt C:\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}\Microsoft-Windows-MobilePC-Client-Premium-Package-
 net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-MobilePC-Client-Premium-Package-shell-31bf3856ad364e35-amd64-en-defined by the control of 
 US~6.2.9200.16384.cat
          Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
 shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE\} \\ Microsoft-Windows-Mobile PC-Client-Premium-Package ~ 31bf3856ad364e35 ~ amd 64 ~ end of the control of the c
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
         Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                         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 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 amd
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
          Opens:
  00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 Opens:
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-Multilingual-Package-admin~31bf3856ad364e35~amd64~en-defined by the control of the control
 US~6.2.9200.16384.cat
                                                                                                                                          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-
US~6.2.9200.16384.cat
    Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \\ Microsoft-Windows-Multilingual-Package-ds-31bf3856ad364e35-amd64-ended and the second control of the second contro
US~6.2.9200.16384.cat
    Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
 inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Multilingual-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-shell~31bf3856ad364e35~amd64~en-
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
    Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               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:
00C04FC295EE}\Microsoft-Windows-NetFx-
NgenAssemblyExclusionClient~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-Windows-NetFx-Shared-Misc~31bf3856ad364e35~amd64~~6.2.9200.16384.cat \\ Control of the control of t
                                                                C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
 00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                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\}\\ \texttt{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 \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-
HttpNamespace~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
 MsmqActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
PipeActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
 TcpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
     Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Shared-WCF-Windows-NetFx-Windows-NetFx-Shared-WCF-Windows-NetFx-Windows-Windows-NetFx-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-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
 TcpPortSharing~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-Package~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-NetFx-VCRedist-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Windows-Built-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ Microsoft-Windows-NetFx2-0C-Package ~ 31bf3856ad364e35 ~ amd 64 ~ en-US-6.2.9200.16384. cat a constant of the constant of th
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-NetFx2-OC-Package ~31bf3856ad364e35 ~amd 64 ~~ 6.2.9200.16384.cat and 100 control of the c
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package-
redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-NetFx3-0C-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-NetFx3-WCF-OC-Package \\ ^{31b}f3856ad364e35 \\ ^{amd}64 \\ ^{6}.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295FF}\Microsoft-Windows-NetFx4-WCF-US-0C-
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-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \verb+\Microsoft-Windows-ParentalControls-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-ParentalControls-Package-31bf3856ad364e35-amd64-en-100c04FC295EEP] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100c04FC295EEP] \verb+\Micr
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 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
     Opens:
                                                                            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:
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-PlayToManager-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-10cm \\ \sim 10cm \\ \sim 10cm
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-
 00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-windows-31bf3856ad364e35-amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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
     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-Portable-Devices-
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-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\} \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Package \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Windows-Printer-Drivers-Package \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Printer-Drivers-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Printer-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows
US~6.2.9200.16384.cat
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-Printing-Foundation-Package \sim 31bf3856ad364e35-amd64-ended of the control of the control
US~6.2.9200.16384.cat
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-Printing-LocalPrinting-Home-localPrinting-Home-local} \\
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Printing-PremiumTools-Package} \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-31bf3856ad364e35 \\ \sim amd64 \\ \sim en-31bf3856ad364 \\ \sim en-31bf3866ad364 \\ \sim en-31bf38666ad364 \\ \sim en-31bf386664 \\ \sim en-31
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-
      Opens:
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-Professional Edition ~31bf3856ad364e35 ~amd 64 ~~ 6.2.9200.16384. cat a constant of the co
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PsuedoTool-HashIDSpy-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-RasCMAK-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                                            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:
Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-RasRip-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim 6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ Microsoft-Windows-RDC-Package ~31bf3856ad364e35 \\ -amd64 \\ -en-US-6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~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\} \\ \mbox{Microsoft-Windows-Redhawk-v1.0-package-31bf3856ad364e35-amd64--6.2.9200.16384.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364e35-amd64--6.2.9200.16384.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364e35-amd64--6.2.9200.0646.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.9200.0646.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.9200.0646.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf3856ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf386ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf386ad364--6.2.0046.cat} \\ \mbox{Continuous-Redhawk-v1.0-package-31bf386ad364--6.2
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ \ Microsoft-Windows-Remote Assistance-Package-Client \sim 31bf3856ad364e35 \sim amd 64 \sim ended to the contract of the contract of
US~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
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
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
LanguagePack~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-RotMgr-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-US \\ \sim 6.2.9200.16384. cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-Search Engine-Client-Package-base \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim ended \\
US~6.2.9200.16384.cat
      Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                            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
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 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
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-Secure Startup-Package \\ ^{31bf3856ad364e35} \\ \ ^{amd64} \\ \ ^{en-package} \\ \ ^{31bf3856ad364e35} \\ \ ^{31bf386ad364e35} \\ \ ^{31bf386ad
US~6.2.9200.16384.cat
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
00C04FC295EE\} \\ Microsoft-Windows-Secure Startup-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~6.2.9200.16384.cat \\ ~6.2.9200.cat \\ ~6.2.9200.cat \\ ~6.2.9200.cat \\ ~6.2.9200.cat \\ 
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-APPXLOB-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-OCUR-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                    C: \verb|\windows\system32\catroot| F750E6C3-38EE-11D1-85E5-\\
 00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 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
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ Microsoft-Windows-ShareMedia-Control Panel-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~endows-ShareMedia-Control Panel-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~a
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:\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-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: \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}\Microsoft-Windows-Shell-HomeGroup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \backslash {\tt Microsoft-Windows-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-SoundThemes-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Shell-Wallpaper-Common-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
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-
00C04FC295EE\} \\ \ Microsoft-Windows-SKU-Foundation-Package-admin-31bf3856ad364e35-amd64-en-defined by the control of the con
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-
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 \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endown 
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}\Microsoft-Windows-SKU-Foundation-Package-com~31bf3856ad364e35~amd64~en-
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-
        Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
00C04FC295EE\} \\ \ Microsoft-Windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~en-decomposition and the second state of the second state o
US~6.2.9200.16384.cat
         Opens:
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
         Opens:
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                        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:
US~6.2.9200.16384.cat
    Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
    Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00Co4FC295EE \} \\ \ Microsoft-Windows-SKU-Foundation-Package-multimedia \sim 31bf3856ad364e35 \sim amd 64 \sim en-block \ Archive the control of the 
US~6.2.9200.16384.cat
                                                                        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\} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-net-} 31bf3856ad364e35 \\ \mbox{-amd} 64 \\ \mbox{-en-package-net-} 31bf3856ad364e35 \\ \mbox{-en-package-net-} 31bf3866ad364e35 \\ \mbox{-en-package-net-} 31bf3866ad364e35 \\ \mbox{-en-package-net-} 31bf3866ad364e35 \\ \mbox{
US~6.2.9200.16384.cat
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-printscan~31bf3856ad364e35~amd64~en-
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
                                                                        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-
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-
US~6.2.9200.16384.cat
                                                                        C:\Windows\System32\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-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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-
US~6.2.9200.16384.cat
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~en-
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
                                                                        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\} \\ Microsoft-Windows-SnippingTool-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~6.2.9200.16384.cat
    Opens:
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-SNMP-Package - 31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat \\ Cathering a contraction of the contraction of
                                                                        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-
00C04FC295EE}\Microsoft-Windows-SpeechRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ \mbox{Microsoft-Windows-StorageService-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim endown \\ 
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-
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 \\ ^a6.2.9200.16384.cat
       Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \\ Microsoft-Windows-Telnet-Client-Package \\ \sim 31bf3856ad364e35 \\ \sim amd \\ 64 \\ \sim 6.2.9200.16384. \\ categorian \\ categori
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-Telnet-Server-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim 
US~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE\} \\ Microsoft-Windows-Telnet-Server-Package ~ 31bf3856ad364e35 ~ amd 64 ~ ~ 6.2.9200.16384. cat a constant of the constant of th
                                                                                                         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 ~31bf3856ad364e35 ~amd64 ~en-defined and the services of the service
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-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
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                         C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-TFTP-Client-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                                         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
      Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
       Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb|\Microsoft-Windows-WebcamExperience-Package-31bf3856ad364e35-amd64-en-defined by the control of the control 
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-
      Opens:
00C04FC295EE\} \\ Microsoft-Windows-WindowsFoundation-LanguagePack-Package \\ ^31bf3856ad364e35\\ ^amd64\\ ^en-Control \\ ^abcdeficies \\ ^abcdefi
US~6.2.9200.16384.cat
      Opens:
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
.00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
      Opens:
                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
```

```
Opens:
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                             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:
Opens:
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-WinSATMediaFiles-\\
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-WMPNetworkSharingService-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Packa
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-WMPNetworkSharingService-Package-31bf3856ad364e35-amd64-ended from the control of the cont
US~6.2.9200.16384.cat
     Opens:
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~amd64~en-
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
    Opens:
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\ntexe.cat
                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\ntpe.cat
                                                                             C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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-
    Opens:
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\} \verb|\windows-Defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364e35-amd64-en-defender-Group-Policy-Package-31bf3856ad364-amd64-en-defender-Group-Policy-Package-31bf3856ad364-amd64-en-defender-Group-Policy-Package-31bf3856ad364-amd64-en-defender-Group-Policy-Package-31bf3856ad364-amd64-en-defender-Group-Policy-Package-31bf3856ad364-amd64-en-defender-Group-Policy-Package-31bf3856ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Policy-Package-31bf3866ad364-amd64-en-defender-Group-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolicy-Bolic
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}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                             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-
    Opens:
00C04FC295EE}\windows-legacy-whql.cat
                                                                             C:\Windows\System32\kerberos.dll
     Opens:
     Opens:
                                                                             C:\Windows\System32\wlanapi.dll
    Opens:
                                                                             C:\Windows\System32\wlanhlp.dll
    Opens:
                                                                             C:\Windows\System32\SubscriptionMgr.dll
     Opens:
                                                                             C:\Windows\System32\wevtapi.dll
     Opens:
                                                                             C:\Windows\System32\netcfgx.dll
    Opens:
                                                                             C:\Windows\Inf
     Opens:
                                                                             C:\Windows\Inf\netcfgx.0.etl
                                                                             C:\Windows\System32\winevt\Logs\Microsoft-Windows-
     Opens
Wcmsvc%40perational.evtx
     Opens:
                                                                             C:\Windows\System32\dpapisrv.dll
                                                                             C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
     Opens:
DPAPI%4Operational.evtx
    Opens:
                                                                             C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
DPAPI%4BackUpKeySvc.evtx
                                                                             C:\Windows\System32\wlansvc.dll
    Opens:
                                                                             {\tt C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-Windows-WLAN-logs\Microsoft-WINDow-log-\Microsoft-WINDow-log-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-WINDow-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-\Microsoft-
     Opens:
AutoConfig%4Operational.evtx
     Opens:
                                                                             C:\
     Opens:
                                                                             C:\Windows\Temp
     Opens:
                                                                             C:\Windows\Temp\ToggleService32.exe\
                                                                             C:\Windows\System32\dps.dll
     Opens:
```

```
Opens:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
DPS%40perational.evtx
                         C:\Windows\System32\diagperf.dll
 Opens:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-
 Opens:
Performance%40perational.evtx
 Opens:
                         C:\Windows\Svstem32\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
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
 Opens:
                         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:
                         C:\Windows\System32\catroot2\edb.chk
 Opens:
                         C:\Windows\System32\catroot2\edb.log
 Opens:
 Opens:
                         C:\Windows\system32\CatRoot2\res1.log
 Opens:
                         C:\Windows\system32\CatRoot2\res2.log
 Opens:
                         C:\Windows\System32\catroot
 Opens:
                         C:\Windows\System32\sppsvc.exe
 Opens:
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
.00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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-
 Opens:
{\tt OOCO4FC295EE} \verb+\Microsoft-Windows-SKU-Foundation-Package-
ds \sim 31bf3856ad364e35 \sim amd64 \sim 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-
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:
                         C:\Windows\Branding
 Opens:
                         C:\Windows\Branding\Basebrd
 Opens:
                         C:\Windows\System32\en-US\sppsvc.exe.mui
 Opens:
                         C:\Windows\System32\sppobjs.dll
 Opens:
 Opens:
                         C:\Windows\Branding\Basebrd\basebrd.dll
 Opens:
                         C:\Windows\System32\wwapi.dll
 Opens:
                         C:\Windows\System32\wscsvc.dll
                         C:\Windows\System32\dbghelp.dll
 Opens:
                         C:\Windows\System32\wbem\wbemprox.dll
 Opens:
 Opens:
                         C:\Windows\System32\wbemcomn.dll
 Opens:
                         C:\Windows\System32\wbem\wbemsvc.dll
 Opens:
                         C:\Windows\System32\wbem\fastprox.dll
 Opens:
                         C:\Windows\System32\winhttp.dll
                         C:\Windows\Svstem32\wuapi.dll
 Opens:
 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\
                         C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows
 Opens:
                         C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft
 Opens:
 Opens:
                         C:\Windows\ServiceProfiles\LocalService\AppData\Local
 Opens:
                         C:\Windows\System32\wups.dll
 Opens:
                         C:\Windows\System32\userenv.dll
                         C:\Windows\System32\wkscli.dll
 Opens:
                         C:\Windows\System32\ci.dll
 Opens:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Opens:
CodeIntegrity%4Operational.evtx
                         C:\Windows\System32\spp\store\data.dat
 Opens:
 Opens:
                         C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
  Opens:
                         C:\Windows\System32\sppwinob.dll
                         C:\Windows\System32\netapi32.dll
 Opens:
```

```
Opens:
                                     C:\Windows\System32\srvcli.dll
                                     C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
  Opens:
manifest-signed.xrm-ms
  Opens:
                                     C:\Windows\System32\spp\store\cache\cache.dat
  Opens:
                                     C:\Windows\System32\spp\store\tokens.dat
                                     C:\Windows\System32\spp\store\data.dat.tmp
  Opens:
                                     C:\Windows\System32\spp\store
  Opens:
                                     C:\Windows\System32\spp\store\data.dat.bak
  Opens:
                                     C:\Windows\System32\msxml6.dll
  Opens:
  Opens:
                                     C:\Windows\System32\msxml6r.dll
  Opens:
                                     C:\Windows\System32\taskschd.dll
  Opens:
                                     C:\Windows\System32\wscinterop.dll
  Opens:
                                     C:\Windows\System32\wscapi.dll
  Opens:
                                     C:\Windows\System32\wscui.cpl
                                     C:\Windows\System32\wscinterop.dll.123.Manifest
  Opens:
                                     C:\Windows\System32\en-US\wscui.cpl.mui
  Opens:
  Opens:
                                     C:\Windows\System32\werconcpl.dll
  Opens:
                                     C:\Windows\System32\wer.dll
                                     C:\Windows\System32\framedynos.dll
  Opens:
                                     C:\Windows\System32\wercplsupport.dll
  Opens:
                                     C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive
  Opens:
  Opens:
                                     {\tt C: \ProgramData\Microsoft\Windows\WER\ReportArchive}
  Opens:
                                     C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\WER\ERC| \\
  Opens:
                                     C:\Windows\System32\hcproviders.dll
  Opens:
                                     C:\Windows\System32\en-US\hcproviders.dll.mui
                                     C:\Windows\System32\en-US\ActionCenter.dll.mui
  Opens:
  Opens:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
WindowsBackup%4ActionCenter.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
  Opens:
NetworkAccessProtection%4WHC.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows
  Opens:
Defender%4WHC.evtx
  Opens:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
Scheduled%40perational.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
  Opens:
TaskScheduler%4Maintenance.evtx
  Opens:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Control
Panel%40perational.evtx
                                     {\tt C:\Windows\System32\winevt\Logs\Microsoft-Windows-Security-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-SPP-UX-S
  Opens:
Notifications%4ActionCenter.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-
  Opens:
Core%4WHC.evtx
  Opens:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
  Opens:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-
ConnectedAccountState%4ActionCenter.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
  Opens:
UserPnp%4ActionCenter.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-
  Opens:
ManagementAgent%4WHC.evtx
  Opens:
                                     C:\Windows\System32\Actioncenter.dll.3.Manifest
  Writes to:
                                     C:\Windows\SysWOW64\output.txt
  Writes to:
                                     C:\Windows\System32\MsDtc\Trace\dtctrace.log
  Writes to:
                                     C:\Windows\System32\MsDtc\MSDTC.LOG
                                     C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
  Writes to:
  Writes to:
                                     C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
  Writes to:
{\tt C:\Windows\Service\Profiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg}
  Writes to:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\31df4714b46f5e5ff8248d0fafa3b957 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
                                     C:\Windows\Inf\netcfgx.0.etl
  Writes to:
  Writes to:
                                     C:\Windows\System32\catroot2\edb.log
  Writes to:
                                     C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
00C04FC295EE}\catdb
                                     C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-
  Writes to:
00C04FC295EE}\catdb
                                     C:\Windows\System32\spp\store\data.dat.tmp
  Writes to:
  Reads from:
                                     C:\Windows\SysWOW64\output.txt
  Reads from:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
AppXDeploymentServer%4Operational.evtx
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
  Reads from:
NetworkProfile%4Operational.evtx
  Reads from:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
StoreMgr%4Operational.evtx
  Reads from:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
DeviceSetupManager%4Operational.evtx
  Reads from:
                                     C:\Windows\System32\winevt\Logs\Microsoft-Windows-
UserPnp%4DeviceInstall.evtx
                                     C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
  Reads from:
  Reads from:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
  Reads from:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
                                     C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
  Reads from:
  Reads from:
                                     C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
  Reads from:
                                     C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
```

```
Reads from:
                         C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
 Reads from:
                         C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
 Reads from:
                         C:\Windows\Inf\netcfgx.0.etl
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
Wcmsvc%40perational.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
 Reads from:
DPAPI%4Operational.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-
DPAPI%4BackUpKeySvc.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-
AutoConfig%4Operational.evtx
 Reads from:
                         C:\Windows\Temp\ToggleService32.exe
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-
DPS%4Operational.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-
Performance%40perational.evtx
                         C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
 Reads from:
00C04FC295EE}\catdb
 Reads from:
                         C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\catdb
 Reads from:
                         C:\Windows\System32\catroot2\edb.log
                         C:\Windows\System32\catroot2\edb.chk
 Reads from:
                         C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
 Reads from:
 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
                         C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
 Reads from:
manifest-signed.xrm-ms
 Reads from:
                         C:\Windows\System32\spp\store\cache\cache.dat
 Reads from:
                         C:\Windows\System32\spp\store\tokens.dat
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Reads from:
WindowsBackup%4ActionCenter.evtx
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
 Reads from:
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
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-
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
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-
 Reads from:
Core%4WHC.evtx
 Reads from:
                         C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx
```

Network Events

UserPnp%4ActionCenter.evtx

ManagementAgent%4WHC.evtx

ConnectedAccountState%4ActionCenter.evtx

Reads from:

Reads from:

Reads from:

Creates kev:

Deletes:

DNS query:	WPAD	
Connects to:	10.74.12.255:138	
Connects to:	10.74.12.255:137	
Sends data to:	10.74.12.255:138	
Sends data to:	10.74.12.255:137	
Receives data from:	10.74.12.100:138	
Receives data from:	10.74.12.100:137	

C:\Windows\System32\spp\store\data.dat.tmp

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-

C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-

C:\Windows\System32\winevt\Logs\Microsoft-Windows-

Windows Registry Events		
Creates key:	<pre>HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-</pre>	
linklocal\linkloca	l_ff00::%12/8	
Creates key:	HKCU\software\classes\local settings\muicache\13\52c64b7e	
Creates key:	HKCU\software\classes\local settings\muicache	
Creates key:	HKLM\software\classes	
Creates key:	<pre>HKLM\system\currentcontrolset\services\vss\diag\registry writer</pre>	
Creates key:	HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer	
Creates key:	<pre>HKLM\system\currentcontrolset\services\vss\diag\asr writer</pre>	
Creates key:	HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization	
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	
Creates key:	HKLM\system\currentcontrolset\control\stillimage	
Creates key:	<pre>HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll</pre>	
Creates key:	<pre>HKLM\system\currentcontrolset\services\nativewifip\parameters</pre>	
Creates key:	HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters	
Creates key:	HKLM\system\currentcontrolset\services\nativewifip	
Creates key:	HKLM\system\currentcontrolset\services\ndisuio	
Creates key:	<pre>HKLM\software\microsoft\windows nt\currentversion\networklist\nla\cache</pre>	

HKLM\software\microsoft\windows

```
nt\currentversion\networklist\nla\cache\intranet
                           HKLM\software\microsoft\windows
 Creates key:
nt\currentversion\networklist\nla\cache\intranet\
                           HKU\s-1-5-21-1923240461-1905901954-2556564120-
 Creates key:
1001\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant\store
 Creates kev:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
 Creates key:
                           HKLM\svstem\wpa
                           HKLM\software\microsoft\security center\svc\vol
 Creates key:
                           HKLM\software\microsoft\security center
 Creates key:
 Creates key:
                           HKLM\software\microsoft\security center\svc
 Creates key:
                           HKLM\software\microsoft\wbem\cimom
 Creates key:
                           HKLM\software
 Creates key:
                           HKLM\software\microsoft
 Creates key:
                           HKLM\software\microsoft\wbem
                           HKLM\system\currentcontrolset\services\sharedaccess\epoch
 Creates kev:
 Creates key:
                           HKLM\software\microsoft\security center\monitoring
 Creates key:
                           HKLM\software\microsoft\windows\currentversion\policies\system
 Creates key:
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
 Creates key:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ action+ \\
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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
                          HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100
 Creates key:
                           HKCU\software\microsoft\windows\windows error reporting
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4\}.check.0
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\startupnotify
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0
 Creates kev:
                           HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
center \verb|\providers| eventlog \verb|\dab69a6a-4d2a-4d44-94bf-e0091898c881| 
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
 Creates key:
                           HKCU\software\microsoft\windows\currentversion\action
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:
                           HKCU\software\microsoft\windows\currentversion\action
center \verb|\checks|{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
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
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key
center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100
 Creates key:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center \verb|\providers| \{2374911b-b114-42fe-900d-54f95fee92e5\}|
 Creates kev:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010
                           HKCU\software\microsoft\windows\currentversion\action
 Creates kev:
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
                           HKCU\software\microsoft\windows\currentversion\action
 Creates key:
center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100
 Deletes value:
                           HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
 Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
```

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

Deletes value:

Deletes value:

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

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

Deletes value:

55779daa70e9}[dhcpsubnetmaskopt]

Deletes value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus tcpip \setminus parameters \setminus tcpip \setminus t$

55779daa70e9}[dhcpdefaultgateway]

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

87b7-55779daa70e9}[dhcpnetbiosoptions]

HKLM\software\microsoft\wow64

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

options\conhost.exe

Opens key: HKLM\svstem\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

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

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

Opens key: HKCII\

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

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens kev: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} compatibility 32$ Opens key: Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ ime compatibility$

Opens key: HKLM\system\currentcontrolset\control\cmf\config

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows

Opens key: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\microsoft\oleaut

Opens key: HKLM\software\microsoft\windows nt\currentversion\console\truetypefont Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen

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

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

 ${\tt HKLM \ } \dot{\tt microsoft \ } sqmclient \backslash windows$ Opens key:

Opens kev: HKLM\system\currentcontrolset\control\nls\sorting\ids Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: ${\tt HKCU \backslash console \backslash \% system root \%_temp_toggleservice 32.exe}$ Opens key: HKCU\console\%systemroot%\temp\toggleservice32.exe Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens kev: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts HKLM\system\currentcontrolset\control\nls\language groups Opens key: Opens kev: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\directmanipulation}} \\$ Opens key: Opens key:

HKLM\software\microsoft\windows\windows error reporting\wmr

Opens key: Opens key:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{\mathbb{N} indows \current version \side by side \label{lem:hklm} } as sembly storage roots. The software \mbox{\mathbb{N} indows \current version \side by side \side \si$

Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

HKLM\system\currentcontrolset\control\lsa Opens key:

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

Opens key: HKLM\software\microsoft\ctf\

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens kev: HKCU\software\microsoft\windows\currentversion\policies\explorer

HKLM\system\currentcontrolset\control\terminal server Opens kev: Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

HKLM\software\microsoft\windows Opens kev: 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 Opens key: HKLM\system\setup Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc HKLM\software\policies\microsoft\windows nt\rpc Opens key: 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 kev: HKLM\software\microsoft\windowsruntime\clsid Opens key: $HKLM \ software \ microsoft \ windows runtime \ clsid \ \{d6015ec3-fa16-4813-9ca1-481$ 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 HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprocserver32 Opens key: Opens key: Opens key: $HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\nprochandler$ Opens key: HKLM\system\currentcontrolset\control\mui\settings Opens key: HKCR\appid\alg.exe HKLM\software\microsoft\ole\appcompat Opens key: Opens key: $HKLM \ software \ \verb|microsoft| cryptography \ defaults \ \verb|provider| \verb|microsoft| strong| \\$ cryptographic provider Opens key: HKLM\software\policies\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography\offload Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046} Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKLM\software\microsoft\rpc\extensions Opens key: ef9508e6a337} Opens kev: $HKCR \land ctivatable classes \land clsid \land \{f8ade1d3-49df-4b75-9005-ef9508e6a337\}$ HKCR\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337} Opens key: HKCR\wow6432node\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337} Opens kev: Opens key: HKCU\software\classes\activatableclasses\clsid Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{3ceb5509 - c1cd - 432f - 9d8f - 9d$ 65d1e286aa80} Opens key: $HKCR \ activatable classes \ \ \ \{3ceb5509-c1cd-432f-9d8f-65d1e286aa80\}$ Opens key: HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80} HKCR\wow6432node\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80} Opens key: Opens key: cd9a10ecd7d1} Opens key: HKCR\activatableclasses\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1} HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1} Opens key:

Opens kev:

HKCR\wow6432node\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}

Opens key

c117c14c429e}

Opens key: Opens kev:

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

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

Opens key:

920843d40be5}

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

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

Opens key: HKCR\wow6432node\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}

HKLM\software\microsoft\windowsruntime\clsid\{6f9942c9-c1b1-4ab5-93da-Opens kev: 6058991dc8f3}

Opens kev: $HKCR \land ctivatable classes \land clsid \land \{6f9942c9-c1b1-4ab5-93da-6058991dc8f3\}$

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

 $HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{6f9942c9 - c1b1 - 4ab5 - 93da - 6058991 \\ dc8f3\}$ Opens key:

Opens key: $HKLM \ software \ microsoft \ windows runtime \ clsid \ \{bc9b54ab-7883-4c13-909f-1884ab-788$

033d03267990}

Opens key:

Opens key: HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}

Opens key: HKCR\wow6432node\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}

Opens key:

7dc40d304059}

Opens key: HKCR\activatableclasses\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}

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

Opens kev: HKCR\wow6432node\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}

Opens kev: HKLM\software\microsoft\alg\isv Opens key: HKLM\software\microsoft\msdtc\tracing Opens key: HKLM\software\microsoft\msdtc\tracing\sources Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash msdtc \backslash tracing \backslash output}$

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

Opens key: HKLM\software\microsoft\msdtc

Opens key: HKCR\cid.local

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

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

Opens key: HKCR\svcid.local

Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464 HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\host Opens key: Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\clsid

HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider Opens key: Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties

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

```
Opens key:
                                                                                                          HKCR\cid.local\15546232-d044-45d4-88a8-
0b84583f2fe1\customproperties\log\size
                                                                                                          HKLM\software\microsoft\msdtc\mtxoci
        Opens key:
       Opens key:
                                                                                                          HKLM\software\microsoft\msdtc\security
       Opens key:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\asr\restoresession
                                                                                                          HKCR\cid.local\15546232-d044-45d4-88a8-
       Opens kev:
0b84583f2fe1\customproperties\log\path
                                                                                                        HKLM\software\microsoft\windows
      Opens kev:
nt\currentversion\tracing\msdtc\loggingoptions
      Opens key:
                                                                                                          HKLM\svstem\currentcontrolset\control\minint
       Opens key:
                                                                                                          Opens key:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules
       Opens key:
                                                                                                          HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions
                                                                                                          \label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint \end{tabular} in th
        Opens key:
       Opens key:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion
       Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac
       Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\description
      Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\svcid
       Opens key:
                                                                                                          HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464
       Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host
       Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid
      Opens key:
                                                                                                          HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
       Opens key:
                                                                                                          HKCR \land cid. local \land 4452c425 - ad2f - 4cde - b895 - 734b166ac4ac \land protocol
       Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint
       Opens key:
                                                                                                          HKCU\control panel\international
       Opens key:
                                                                                                          HKLM\software\microsoft\rpc\securityservice
       Opens key:
                                                                                                          HKLM\system\currentcontrolset\control\securityproviders
       Opens key:
                                                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache
       Opens key:
                                                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
       Opens key:
                                                                                                          HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties
       Opens key:
                                                                                                          HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties\dac
       Opens kev:
                                                                                                          HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc
       Opens key:
       Opens kev:
                                                                                                          HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc\description
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab
       Opens key:
       Opens key:
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\description
       Opens key:
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid
       Opens key:
                                                                                                          HKLM \verb|\system| current control \verb|\sta| access providers
       Opens key:
                                                                                                          HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
       Opens key:
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host
       Opens key:
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid
       Opens key:
                                                                                                          HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider
       Opens key:
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol
                                                                                                          HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\endpoint
       Opens key:
                                                                                                          Opens kev:
b913c40c9cd4}
                                                                                                          HKCR\activatableclasses\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
       Opens kev:
       Opens key:
                                                                                                          HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
       Opens key:
                                                                                                          HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
       Opens key:
                                                                                                          HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\ \ \ inprocserver 32
       Opens key:
                                                                                                          \label{lem:hkcr} $$HKCR\clsid{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler 32$
       Opens key:
                                                                                                          HKLM\software\policies\microsoft\windows nt\reliability
       Opens kev:
       Opens key:
                                                                                                          HKLM\hardware\description\system\centralprocessor\0
      Opens key:
                                                                                                          HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
appxdeploymentserver/operational
       Opens key:
HKLM \software \mbox{\tt microsoft-windows-current} version \mbox{\tt winevt-channels-microsoft-windows-current} version \mbox{\tt windows-current} version \mbox{\tt windo
appxdeploymentserver/operational
       Opens key:
                                                                                                        \label{lem:hklmsystem} \verb|HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-lementary | lementary | lementary
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-currentversion\channels\microsoft-windows-currentversion\channels\micr
networkprofile/operational
      Opens key:
                                                                                                        HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
kernel-storemgr/operational
      Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus winevt \setminus channels \setminus microsoft \cdot windows \cdot kernel-to-soft \setminus windows \cdot kernel-to-soft \cdot windows 
storemgr/operational
                                                                                                          HKLM\svstem\currentcontrolset\services\eventlog\microsoft-windows-
      Opens key:
devicesetupmanager/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
devicesetupmanager/operational
        Opens key:
                                                                                                          HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
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-currentversion\channels\microsoft-windows-currentversion\channels\micr
userpnp/deviceinstall
       Opens key:
                                                                                                          HKU \verb|\|.default\| software \verb|\| policies \verb|\| microsoft\| windows \verb|\| safer\| code identifiers
                                                                                                          HKU\.default\control
       Opens kev:
panel\desktop\muicached\machinelanguageconfiguration
      Opens key:
                                                                                                         HKU\.default\software\policies\microsoft\control panel\desktop
       Opens key:
                                                                                                          \label{thm:local_ham} \begin{tabular}{ll} HKU\label{thm:local_ham} HKU\label{thm:local_ham} AKU\label{thm:local_ham} \end{tabular} AKU\label{thm:local_ham} and \end{tabular} \begin{tabular}{ll} AKU\label{tabular} AKU\lab
       Opens key:
                                                                                                          HKU\.default\control panel\desktop
       Opens key:
                                                                                                          HKU \verb|\|.default\\| control panel\\| desktop\\| muicached
       Opens key:
                                                                                                          HKLM\software\microsoft\windows\currentversion\winevt
       Opens key:
                                                                                                          HKLM\software\microsoft\windows\currentversion\winevt\publishers
```

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-496-a5ba-496-a5ba-496-a5ba-496-a5ba-496-a5ba-496-a5ba-496-a5ba-496-a5
3e3b0328c30d3
     Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e
26931d2012f4}
    Opens kev:
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
    Opens key:
                                                                        HKLM\system\currentcontrolset\services\eventlog\system\service control
manager
    Opens key:
                                                                        HKLM\software\microsoft\windows nt\currentversion\svchost
     Opens key:
                                                                        HKLM\software\microsoft\windows
nt\currentversion\svchost\localservicepeernet
    Opens key:
HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile
                                                                        HKLM\system\currentcontrolset\services
    Opens key:
     Opens kev:
                                                                        HKLM\system\currentcontrolset\services\p2pimsvc
    Opens key:
                                                                        HKLM\system\currentcontrolset\services\p2pimsvc\parameters
    Opens key:
                                                                        HKLM\software\microsoft\windows nt\currentversion\diagnostics
    Opens key:
                                                                        HKLM\software\microsoft\windows nt\currentversion\winlogon
     Opens key:
                                                                        HKLM\software\policies\microsoft\windows\system
    Opens key:
                                                                        HKLM\software\policies\microsoft\peernet
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\pnrpsvc
    Opens key:
                                                                        HKLM\system\currentcontrolset\services\pnrpsvc\parameters
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\winsock2\parameters
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1-3a1fc5ac
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog\2c69d9f1
    Opens key:
HKLM \verb|\system| current control set \verb|\services| winsock2 \verb|\parameters| protocol\_catalog9 | leading to the control set \verb|\system| current control set \|\system| current control set \|
    Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000001
    Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\0000000000003
    Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000004
    Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000007
    Opens kev:
Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ possible \ and \ protocol\_catalog \ possible \ protocol\_catalog \ pro
    Opens key:
Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
    Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000005
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000006
     Opens kev:
                                                                        HKLM\svstem\currentcontrolset\services\winsock\parameters
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
    Opens key:
                                                                        HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
    Opens key:
                                                                        HKLM\system\currentcontrolset\services\winsock\setup migration\providers
    Opens kev:
                                                                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
                                                                        HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
    Opens key:
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
    Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus interfaces \setminus \{a04231f6-42eb-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b8
25b8d56dd1d8}
```

```
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
  Opens key:
HKLM \ system \ current controls et \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-805d63-805d63-805d63-805d63-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d648-805d648-805d648-805d64-805d648-805d648-805d648-805d64-805d648-805d648-805d648-805d648-805d64
55779daa70e9}
  Opens kev:
806e6f6e6963}
   Opens key:
                                       HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
                                       HKLM\software\microsoft\sqmclient
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp
  Opens key:
                                       HKLM\software\policies\microsoft\peernet\pnrp\ipv6-linklocal
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal
  Opens key:
  Opens key:
                                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
                                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
  Opens key:
  Opens key:
                                       {\tt HKLM \ } system \verb| current control set \verb| services \verb| crypt32| \\
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype 0
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
                                       HKLM\software\microsoft\cryptography\oid\encodingtype 1
  Opens key:
  Opens kev:
                                       {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \\
1\certdllopenstoreprov
                                       HKLM\software\microsoft\crvptographv\oid\encodingtvpe
  Opens kev:
0\cryptdlldecodeobjectex
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex
                                       {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\
  Opens key:
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
  Opens key:
                                      HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
                                      {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
  Opens key:
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
                                      HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key
1\crvptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
  Opens key
                                      {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
  Opens key
                                      HKLM\software\microsoft\cryptography\oid\encodingtype
1\crvptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
                                       {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ oid \verb|\ encoding type \\
  Opens key:
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
  Opens key:
                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ msasn1
                                       HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
  Opens kev:
schannel cryptographic provider
                                       HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
                                       HKLM\software\microsoft\cryptography\deshashsessionkeybackward
  Opens kev:
  Opens key
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo
                                       {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\
  Opens key
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7
  Opens key:
                                       {\tt HKLM \ } system \verb|\ current control \ \verb|\ mui \ \verb|\ string caches \ ettings \\
  Opens key:
                                       HKCU\software\classes\local settings\muicache\13\52c64b7e
  Opens key:
                                       HKCU\software\classes\local settings\muicache
  Opens key:
                                       {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ oid \verb|\ encoding type \\
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
  Opens key:
                                      HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7
                                      HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens kev:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7
                                      {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \\
  Opens kev:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.76.6.1!7
  Opens key
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllencodepublickeyandparameters
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
1\cryptdllencodepublickeyandparameters
  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
                                       {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\
  Opens key:
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.1.1
                                       {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ oid \verb|\ encoding type \\
  Opens key
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.1
  Opens key:
                                       {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.11
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.12
  Opens key:
                                       HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.2
```

```
Opens key:
                                                                      HKLM\software\microsoft\cryptography\oid\encodingtype
 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.3
                                                                      {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ oid \verb|\ encoding type \\
     Opens key:
 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.4
    Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options
    Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe
     Opens key:
                                                                      HKLM\system\currentcontrolset\control\print
    Opens key:
                                                                      HKCR\clsid
    Opens key:
                                                                      HKLM\software\policies\microsoft\windows nt\printers
    Opens key:
                                                                      HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
    Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
                                                                      HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
     Opens key:
     Opens key:
                                                                      HKLM\software\microsoft\telemetryclient\throttlestore\sqm
     Opens key:
                                                                      HKLM\software\microsoft\telemetryclient\throttlestore
     Opens key:
                                                                      HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
                                                                      HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
    Opens key:
     Opens key:
                                                                      HKLM\software\microsoft\telemetryclient\samplestore\sqm
    Opens key:
HKLM \ software \ microsoft \ telemetry client \ throttlestore \ sqm \ windows \ winsqm 8 \ 13238528
    Opens key:
HKLM \ software \ microsoft \ telemetry client \ sample store \ sqm \ windows \ winsqm 8 \ 13238528
     Opens key:
HKLM \ software \ microsoft \ telemetry client \ throttlestore \ sqm \ win sqm 8 \ 13238784
    Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
     Opens key:
                                                                      HKLM\system\currentcontrolset\services\lmhosts
     Opens key:
                                                                      HKLM\system\currentcontrolset\services\lmhosts\parameters
     Opens key:
                                                                      HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
    Opens key:
                                                                      HKCR\appid\vssvc.exe
                                                                      HKLM\software\microsoft\windowsruntime\clsid\{e579ab5f-1cc4-44b4-bed9-
     Opens kev:
de0991ff0623}
                                                                      HKCR\activatableclasses\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
     Opens kev:
                                                                      HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
     Opens key:
                                                                      HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\treatas
     Opens key:
    Opens key:
                                                                      HKCR \verb|\clsid|{e579ab5f-1cc4-44b4-bed9-de0991ff0623} \verb|\inprocserver32|
     Opens key:
                                                                      HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
     Opens key:
                                                                      \label{lem:hkcr} \begin{tabular}{ll} HKCR\clsid\\ e579ab5f-1cc4-44b4-bed9-de0991ff0623\\ \end{tabular} \begin{tabular}{ll} \be
     Opens key:
                                                                      6c6d4570e40f}
     Opens key:
                                                                      HKCR\activatableclasses\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
     Opens key:
                                                                      HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
                                                                      HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\treatas
    Opens key:
                                                                      HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprocserver32
     Opens kev:
     Opens key:
                                                                      HKCR \ clsid \ \{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f\} \ in prochandler
     Opens key:
    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 \{4e14fba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-11d1-9964-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e22-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-2e24ba2-14e4ba2-14e4ba2-2e24ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4ba2-14e4b
00c04fbbb345}
                                                                      HKCR\activatableclasses\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
     Opens key:
     Opens key:
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
     Opens key:
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
     Opens key:
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
    Opens key:
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
     Opens kev:
                                                                      HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{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
    Opens key
00c04fb926af}
     Opens key:
                                                                      HKCR \land ctivatable classes \land clsid \land \{1be1f766-5536-11d1-b726-00c04fb926af\}
     Opens key:
                                                                      HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
     Opens key:
                                                                      HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
     Opens key:
                                                                      HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\
     Opens key:
                                                                      \label{lem:hkcr} \begin{tabular}{ll} HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\\\ \label{lem:hkcr} \end{tabular}
                                                                      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\}\ proxystubclsid 32
    Opens key:
                                                                      HKLM\software\microsoft\windowsruntime\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}
                                                                      HKCR \ activatable classes \ \ clsid \ \ \{64b8f404-a4ae-11d1-b7b6-00c04fb926af\}
     Opens kev:
     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}\nprochandler32
     Opens key:
                                                                      HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler
     Opens key:
                                                                      HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}
                                                                      HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
     Opens key:
    Opens key:
                                                                      HKCR\interface\{00000100-0000-0000-0000000000046}
     Opens key:
                                                                      HKCR\interface\{00000100-0000-0000-c000-00000000046}\proxystubclsid32
    Opens key:
                                                                      HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}
     Opens key:
                                                                      HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
    Opens kev:
                                                                      HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{7542e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-11d1-88f9-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1442e960-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79c7-1460-79
0080c7d771bf}
                                                                      Opens key:
     Opens key:
                                                                      HKCR \ clsid \ \{7542e960-79c7-11d1-88f9-0080c7d771bf\}
     Opens key:
                                                                      HKCR\clsid{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
     Opens key:
                                                                      HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\clsid\{7542e96
                                                                      Opens key:
```

```
Opens key:
                                                  HKCR \ clsid \ \{7542e960-79c7-11d1-88f9-0080c7d771bf\} \ \ in prochandler
   Opens key:
                                                  HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}
   Opens key:
                                                  HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
   Opens key:
   Opens key:
                                                  HKLM\system\currentcontrolset\services\vss\diag\asr writer
   Opens kev:
                                                  HKLM\svstem\currentcontrolset\services\vss\diag\shadow copv optimization
writer
   Opens key:
                                                  HKLM\system\currentcontrolset\services\eventlog\application\vss
   Opens key:
Opens key
Opens key:
HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
                                                  Opens key:
   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
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-
   Opens key:
a3cc-00a0c9223196}
   Opens key:
                                                  HKLM\software\microsoft\windows\currentversion\audio
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\svchost\wersvcgroup
   Opens key:
                                                  HKU\.default\control panel\international
   Opens key:
                                                  HKLM\system\currentcontrolset\services\wersvc
   Opens key:
                                                  HKLM\system\currentcontrolset\services\wersvc\parameters
   Opens key:
                                                  HKLM\software\microsoft\windows\windows error reporting
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\svchost\imgsvc
   Opens key:
                                                  HKLM\system\currentcontrolset\services\stisvc
   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
                                                  HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
   Opens key:
                                                  Opens kev:
0060081ed811}
   Opens key:
                                                  HKCR\activatableclasses\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
                                                  HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
   Opens key:
   Opens key:
                                                  HKCR \ clsid \ \{a1f4e726-8cf1-11d1-bf92-0060081ed811\} \ treat as
   Opens key:
                                                  HKLM \verb|\system| current controlset| control \verb|\stillimage| fake devices|
   Opens key:
                                                  HKLM\software\microsoft\windows\currentversion\setup
   Opens key:
                                                  HKLM\software\microsoft\windows\currentversion
                                                  HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprocserver32
   Opens key:
   Opens key:
                                                  HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler32
   Opens key:
                                                  HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{6bdd1fc6-810f-11d0-
   Opens kev:
bec7-08002be2092f}
                                                  Opens kev:
8ec92617e599}
   Opens key:
                                                  HKCR\activatableclasses\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
   Opens key:
                                                  HKCR\clsid\b6c292bc-7c88-41ee-8b54-8ec92617e599
   Opens key:
                                                  HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\treatas
   Opens key:
                                                  HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\ \ inprocserver 32
   Opens key:
                                                  \label{lem:hkcr} $$ HKCR\clsid{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler 32 $$
   Opens key:
                                                  HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\ \ in prochandler
                                                  HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{a1e75357 - 881a - 419e - 83e2 - 419e - 83
   Opens key:
bb16db197c68}
                                                  HKCR \ activatable classes \ \ clsid \ \{a1e75357-881a-419e-83e2-bb16db197c68\}
   Opens key:
                                                  HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
   Opens kev:
                                                  HKCR\wow6432node\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
   Opens key:
   Opens kev:
                                                  HKLM\system\currentcontrolset\control\stillimage\mscdevicelist
                                                  HKLM\system\currentcontrolset\control\stillimage
   Opens key:
   Opens key:
                                                  {\tt HKLM \ } system \verb|\ current control \verb|\ stillimage \verb|\ events|
   Opens key:
                                                  \label{lem:ham} \verb|HKLM\| system \land control \land stillimage \land events \land connected \\
   Opens key:
HKLM \ system \ control set \ liming events \ connected \ \{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-4ea6
6c15f82b5905}
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm \system \current control \stillimage \space{-0.05cm} events \space{-0.05cm} disconnected
   Opens key:
                                                  HKLM\system\currentcontrolset\control\stillimage\events\emailimage
   Opens key:
759eb35cdf9a}
                                                  HKLM\svstem\currentcontrolset\control\stillimage\events\faximage
   Opens kev:
   Opens kev:
759eb35cdf9a}
   Opens key:
                                                  HKLM\system\currentcontrolset\control\stillimage\events\printimage
   Opens key:
759eb35cdf9a}
   Opens key:
                                                  HKLM\system\currentcontrolset\control\stillimage\events\scanbutton
   Opens key:
HKLM\system\currentcontrol\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}
   Opens key:
759eb35cdf9a}
   Opens kev:
7105fd3b53b1}
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}
                      HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent
 Opens key:
 Opens key:
                      HKLM\system\currentcontrolset\control\stillimage\serversettings
                      HKLM\system\currentcontrolset\services\nativewifip
 Opens key:
 Opens key:
                      HKLM\system\currentcontrolset\services\nativewifip\parameters
                      HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
 Opens kev:
                      HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
 Opens key:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
                      HKLM\system\currentcontrolset\services\ndisuio
 Opens key:
 Opens key:
Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
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\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0007\linkage
 Opens key:
                      HKLM\system\currentcontrolset\enum\root\ms ndiswanipv6\0000
                      HKLM\system\currentcontrolset\services\nnetsecl\parameters
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0006
 Opens key:
                      HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005
 Opens key:
                      08002be10318}\0005\linkage
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage
                      HKLM\system\currentcontrolset\services\wlansvc
 Opens key:
 Opens kev:
                      HKLM\system\currentcontrolset\enum\root\ms pppoeminiport\0000
                      Opens key
08002be10318}\0004
                      Opens key:
08002be10318}\0004\linkage
 Opens key:
                      HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
 Opens key:
                      HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key
08002be10318}\0003
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens kev:
08002be10318}\0003\linkage
                      HKLM\system\currentcontrolset\services\wlansvc\linkage
 Opens key:
 Opens key:
                      HKLM\system\currentcontrolset\services\wlansvc\parameters
 Opens key:
                      HKLM\system\currentcontrolset\control\wmi\security
 Opens key:
                      Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\0011\linkage
                      HKLM\system\currentcontrolset\enum\root\*teredo\0000
 Opens key:
 Opens kev:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0012
 Opens kev:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0012\linkage
                      HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000
 Opens key:
 Opens key:
                      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\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\linkage
                      HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens kev:
08002be10318}
 Opens key:
                      HKLM\software\microsoft\wcmsvc
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008
 Opens key:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Opens key:
08002be10318}\properties
 Opens key:
                      HKLM\software\microsoft\wcmsvc\subscriptionmanager
 Opens key:
                      HKLM\system\currentcontrolset\control\cryptography\providers
 Opens key:
                      HKLM\system\currentcontrolset\control\cryptography\configuration
 Opens key:
                      HKLM\software\microsoft\windowsruntime\clsid\{5b035261-40f9-11d1-aaec-
00805fc1270e}
 Opens key:
                      HKCR\activatableclasses\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
                      HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
 Opens key:
 Opens key:
                      \label{local-condition} HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\ \ treat as
 Opens key:
                      Opens key:
                      Opens key:
```

Opens key: HKLM\system\currentcontrolset\control\network Opens key: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{67d07935-283a-4791-8f8d-4791-8f$ fa9117f3e6f2} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowswcmsvc/operational Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/operational Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowswcmsvc/diagnostic Opens key: $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{windows$}$-windows-$} \noindent \$ wcmsvc/diagnostic Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3} HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3} Opens kev: Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32 $HKCR\interface { dbea162d-04e8-460f-8a0b-4a431715d9a3 } \proxystubclsid32 \\$ Opens key: Opens kev: HKLM\software\policies\microsoft\windows\edgeui HKCU\software\policies\microsoft\windows\edgeui Opens key: Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9} Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9} Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32 HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32 Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowscrypto-dpapi/operational Opens key: dpapi/operational Opens kev: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowscrypto-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-windowscrypto-dpapi/debug Opens key: $HKLM \ software \ microsoft-windows \ - crypto-like \ microsoft-windows \ - crypto-like \$ dpapi/debug Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870d5be7d52d6de} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-wlanautoconfig/operational Opens key: autoconfig/operational Opens key: ${\tt HKLM} \ system \verb|\currentcontrolset\ services \verb|\eventlog\ microsoft-windows-wlan-def} \\$ autoconfig/diagnostic Opens key: $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlandow$ autoconfig/diagnostic HKLM\software\policies\microsoft\windows\appcompat Opens key: Opens kev: HKLM\system\currentcontrolset\control\diagnostics\performance Opens key HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger Opens key: HKCU\software\classes\applications\calc.exe Opens key: HKCR\applications\calc.exe Opens key: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{6bba3851-2c7e-4dea-8f54-4dea-8f$ 31e5afd029e3} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsdiagnosis-dps/debug Opens kev: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/debug Opens key: $\label{local-control} \mbox{HKLM} \mbox{$\tt NSYSTEM} \mbox{$\tt Current control set} \mbox{$\tt Services} \mbox{$\tt NSYSTEM} \mbox{$\tt NSYSTEM}$ diagnosis-dps/operational Opens key: $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -diagnosis-diagnosi$ 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\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosisdps/analytic Opens kev: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsdiagnostics-performance/operational Opens key:

 $\label{lem:hklm} \verb+Kklm \system \current control set \services \$

performance/operational

Opens key:

```
diagnostics-performance/diagnostic
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostics \ -diagnos
performance/diagnostic
                                                                              HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
     Opens key:
 diagnostics-performance/diagnostic/loopback
     Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostic s \ -diagno
performance/diagnostic/loopback
                                                                              HKLM\system\currentcontrolset\services\tcpip\parameters
     Opens key:
      Opens key:
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 kev:
 HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
     Opens key:
                                                                              HKLM\system\currentcontrolset\services\netbt\adapters\{b5105d63-74c6-
 .
4dc1-87b7-55779daa70e9}
      Opens kev:
                                                                              HKLM\svstem\currentcontrolset\services\netbt\parameters
     Opens key:
                                                                              HKLM\system\currentcontrolset\services\dnscache
                                                                              \label{lem:hklm} \verb+Kklm \system \current control set \services \
     Opens key:
     Opens key:
                                                                              HKLM\software\microsoft\ctf\knownclasses
      Opens key:
                                                                              HKLM \verb|\system| current controlset \verb|\services| p2pimsvc \verb|\startoverride|
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\dcomlaunch
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\rpceptmapper
                                                                              HKLM\system\currentcontrolset\services\rpcss
      Opens key:
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\sppsvc
      Opens key:
                                                                              HKU\s-1-5-20
      Opens key:
                                                                              HKLM\system\currentcontrolset\control\session manager\environment
      Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20
      Opens key:
                                                                              HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
 shell folders
                                                                              HKU\s-1-5-20\environment
      Opens key:
      Opens kev:
                                                                              HKU\s-1-5-20\volatile environment
                                                                              HKU\s-1-5-20\volatile environment\0
     Opens key:
     Opens key:
                                                                              \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
 options\sppsvc.exe
      Opens key:
                                                                              \label{lem:hklm} \verb+Kklm \ system \ current control \ session \ manager \ \ quota \ system \ \ s-1-
 5-20
                                                                              HKCR\appid\sppsvc.exe
     Opens key:
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\eventlog\application\software
protection platform service
     Opens kev:
 HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-
 f2bdfea0f156}
                                                                             HKLM\software\microsoft\windows
     Opens key:
 nt\currentversion\softwareprotectionplatform
                                                                              HKLM \ system \ wpa \ 8 dec 0 af 1 - 0341 - 4b93 - 85cd - 72606c 2df 94c - 6p - 1
      Opens key:
      Opens key:
                                                                              HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10
      Opens key:
                                                                              HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11
      Opens key:
                                                                              HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12
      Opens key:
                                                                              HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-13
                                                                              HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14
      Opens kev:
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\wsearch
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\http
      Opens kev:
                                                                              HKLM\svstem\currentcontrolset\services\wmpnetworksvc
```

Opens key: HKLM\system\currentcontrolset\services\winmgmt Opens kev: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ wscsvc|$

Opens key: HKLM\system\currentcontrolset\services\wscsvc\parameters Opens key: $HKLM \setminus system \setminus wpa \setminus 8 dec 0 af 1 - 0341 - 4b93 - 85cd - 72606c 2df 94c - 6p - 15$ Opens key: $HKLM \ system \ wpa \ 8 dec \ 0 af 1 - 0 3 4 1 - 4 b 9 3 - 8 5 c d - 7 2 6 0 6 c 2 d f 9 4 c - 6 p - 16$ Opens key: HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-17 Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18 HKLM\software\microsoft\security center\svc\vol Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19 Opens key:

Opens key: HKLM\software\microsoft\security center\svc

HKLM\software\microsoft\windowsruntime\clsid\{4590f811-1d3a-11d0-891f-Opens key:

00aa004b2e24}

Opens key: HKCR\activatableclasses\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}

HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens kev: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas Opens key:

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:

Opens key: ${\tt HKLM \backslash software \backslash policies \backslash microsoft \backslash system \backslash dnsclient}$ Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2

 $HKLM \ software \ microsoft \ windows runtime \ clsid \ \{8bc3f05e-d86b-11d0-a075-d86b-11d0-a07$ Opens key:

00c04fb68820}

Opens key: HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas Opens kev: Opens key:

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\ \ inprochandler 32$ Opens key: Opens key: $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\ \ in prochandler$ Opens key: $HKCR \ clsid \ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \ local server 32$

Opens key: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver Opens key: $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\elevation$ HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key:

```
Opens key:
                                                         Opens key:
                                                         HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\localserver32
                                                        HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
    Opens key:
00c04fb68820}\localserver
                                                        HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\elevation
    Opens kev:
    Opens key:
                                                         HKCR\unmarshalers\system\{00000339-0000-0000-c000-00000000046}
   Opens key:
                                                         HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
    Opens key:
                                                         HKCR\ interface \ \{f309ad18-d86a-11d0-a075-00c04fb68820\}\ proxystubclsid32
                                                         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 \land ctivatable classes \land clsid \land \{7c857801-7381-11cf-884d-00aa004b2e24\}
    Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
    Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
    Opens key:
                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20
    Opens key:
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
                                                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
    Opens key:
    Opens key:
                                                         HKCR\ clsid \ \ \{7c857801-7381-11cf-884d-00aa004b2e24\} \ \ in prochandler
   Opens key:
                                                         HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
    Opens key:
                                                         HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
   Opens key:
                                                         HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
    Opens key:
                                                         HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
   Opens key:
                                                         ce99a996d9ea}
    Opens key:
                                                         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}\ \ inprocserver 32
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ in prochandler 32
    Opens key:
                                                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler
    Opens key:
    Opens key:
                                                         HKLM\software\microsoft\wbem\cimom
                                                         Opens key:
252725d697ca}
    Opens key:
                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21
    Opens kev:
                                                         HKCR\activatableclasses\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:
                                                         \label{lem:hkcr} $$ HKCR\clsid\\{e7d35cfa-348b-485e-b524-252725d697ca}\inprocserver 32 $$
    Opens key:
                                                         Opens key:
                                                         HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler
                                                         HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}
    Opens key:
    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-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-142-b5fb-1
00104b703efd}
                                                         HKCR\activatableclasses\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}
    Opens key:
    Opens kev:
                                                         HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}
                                                         HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\treatas
```

Opens key: $HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32$ Opens key: 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-c000-000000000046} 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}

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32 Opens key:

00104b703efd}

Opens kev: HKCR\activatableclasses\clsid\{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: $HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\ \ in procserver 32$ Opens key: Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler

Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd} Opens key: Opens key: $HKCR\ interface \ \{423ec01e-2e35-11d2-b604-00104b703efd\}\ proxystubclsid 32$ Opens key: HKLM\software\microsoft\windowsruntime\clsid\{bfe18e9c-6d87-4450-b37c-

e02f0b373803}

HKCR\activatableclasses\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803} Opens kev:

 $\label{local-eq:hkcr} $$ HKCR\clsid_{bfe18e9c-6d87-4450-b37c-e02f0b373803} $$$ Opens kev: Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\treatas Opens key: $HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\\\\inprocserver32$ Opens key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22 Opens key: $HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\\label{line} In prochandler 32$ Opens key: HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprochandler ${\tt HKLM \backslash system \backslash current control \backslash compression}$ Opens kev:

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

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

Opens kev:

9d55-7b8e7f157091}

Opens key:

9d55-7b8e7f157091}\propertybag

Opens key: HKCU\software\microsoft\windows\currentversion\explorer

Opens key:

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

```
Opens key:
                                                    HKCU\software\policies\microsoft\windows\explorer
   Opens key:
Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions' \ '5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder \ '
9afe-ea3317b67173}\propertybag
   Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23
   Opens key:
   Opens key:
                                                    HKLM \ software \ microsoft \ windows \ current version \ window supdate \ trace \ misconstruction \ trace \ misconstruction \ misconstr
   Opens key:
Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\setup
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\service
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\agent
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\au
   Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\auclnt
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cltui
   Opens key:
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cpl
   Opens key:
                                                    Opens key:
                                                    Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\dtastor
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cdm
   Opens key:
                                                    Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\driver
                                                   HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24
   Opens kev:
   Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\comapi
   Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\parser
   Opens key:
Opens key:
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\dnldmgr
   Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\cmpress
   Opens kev:
Opens kev:
Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\offlsnc
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\inv
   Opens key:
                                                    HKLM \ software \ microsoft \ windows \ current version \ windows \ update \ trace \ arp
   Opens key:
                                                    HKLM \ software \ `microsoft\ `windows \ `current version \ `windows update \ `trace' \ trace' \ tra
   Opens key:
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\tracetestmain
   Opens kev:
HKLM \ software \ microsoft \ windows \ current version \ windows \ update \ trace \ trace test threads
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\perf.
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\ws
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\ep
   Opens kev:
   Opens key
HKLM\software\microsoft\windows\currentversion\windowsupdate\trace\wutask
   Opens key:
                                                    HKLM \ software \ microsoft \ windows \ current version \ window supdate \ trace \ mowu
   Opens key:
HKLM \ software \ microsoft \ windows \ current version \ window \ supdate \ trace \ reboot notify
HKLM\software\microsoft\windows\currentversion\windowsupdatesysprepinprogress
   Opens key:
                                                    HKLM\software\policies\microsoft\windows\windowsupdate
   Opens key:
                                                    HKLM\software\policies\microsoft\windows\windowsupdate\au
   Opens key:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\windowsupdate\auto update
                                                    HKCU\software\microsoft\windows\currentversion\policies\windowsupdate
   Opens kev:
   Opens kev:
                                                    HKLM \verb|\software\microsoft\windows\currentversion\windows update \verb|\auto||
update\rebootrequired
   Opens key:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26
   Opens key:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27
   Opens key:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29
   Opens key:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3
   Opens kev:
   Opens key:
4139-a9ba-be0bbbf5b74d\2fb92682-6599-42dc-ae13-bd2ca89bd11c
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30
   Opens kev:
   Opens key:
HKLM\system\currentcontrolset\services\eventlog\application\securitycenter
   Opens key:
                                                    HKLM\software\microsoft\windows\currentversion\policies\system
   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:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33
   Opens key:
                                                    HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4
```

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5

Opens key:

```
Opens key:
                                                                                                                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6
            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\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-
 3937643e37a3}
                                                                                                                                                          HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
          Opens kev:
  codeintegrity/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
 codeintegrity/operational
                                                                                                                                                          \label{lem:hklm} \verb+Kklm \system \current control set \services \
            Opens key:
  codeintegrity/verbose
            Opens key:
 HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
 codeintegrity/verbose
                                                                                                                                                          HKCU\software\microsoft\windows
          Opens key:
 nt\currentversion\softwareprotectionplatform\persistedtsrearmed
                                                                                                                                                          HKCU\software\microsoft\windows
          Opens kev:
 nt\currentversion\softwareprotectionplatform\persistedsystemstate
          Opens key
                                                                                                                                                          HKLM\software\microsoft\windows
  nt\currentversion\softwareprotectionplatform\plugins\modules
                                                                                                                                                          HKLM\software\microsoft\windows
            Opens key
 nt \verb| current version \verb| software protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules \verb| 179b8a65-b0f6-41d9-acea-12006ef9b32a| and the protection platform \verb| plugins \verb| modules modules \verb| modules 
                                                                                                                                                          HKLM\software\microsoft\windows
            Opens key:
 \verb|nt\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 plugins| modules| c42d84662| and the plugins| modules| c42d84662| and the plugins| and the plugins| and the pl
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects
          Opens key:
                                                                                                                                                         HKLM\software\microsoft\windows
 HKLM\software\microsoft\windows
          Opens key:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0
          Opens key:
                                                                                                                                                         HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0
          Opens key:
                                                                                                                                                         HKLM\software\microsoft\windows
 Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/phone/1.0| | the protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/phone/1.0| | the protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/phone/1.0| | the protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/phone/1.0| | the protection platform \verb| objects \verb| msft:rm/algorithm/phone/1.0| | the protection platform \verb| objects | objects \verb| objects | objects | objects | objects | objects | objects |
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009
                                                                                                                                                          HKLM\software\microsoft\windows
          Opens kev:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect
          Opens kev:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
  nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0
                                                                                                                                                          HKLM\software\microsoft\windows
            Opens key:
 \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
 Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0
                                                                                                                                                         HKLM\software\microsoft\windows
          Opens key:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0
          Opens key
                                                                                                                                                         HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0
          Opens key
                                                                                                                                                          HKLM\software\microsoft\windows
 nt \verb|\colored | software protection platform \verb|\colored | plugins \verb|\colored | software protection platform | plugins \verb|\colored | software protection platform | plugins \verb|\colored | software protection | software protection platform | plugins \verb|\colored | software protection | softw
          Opens key
                                                                                                                                                          HKLM\software\microsoft\windows
  nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0
            Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
  nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
  nt \verb|\colored | some of twa reprotection platform \verb|\colored | plugins \verb|\colored | some of the plugins of th
                                                                                                                                                          HKLM\software\microsoft\windows
          Opens key:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0
                                                                                                                                                          HKLM\software\microsoft\windows
          Opens key:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt \verb|\colored | logist | log
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft:spp/licenseacquisition/payloadhandler/spc/1.0| and the plugins objects obje
            Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows
 nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/sequence/1.0| and the protection platform \verb|\plugins| objects ob
          Opens kev:
                                                                                                                                                         HKLM\software\microsoft\windows
 nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/statecollector/pkey| | the following the state of 
                                                                                                                                                         HKLM\software\microsoft\windows
          Opens key:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
                                                                                                                                                         HKLM\software\microsoft\windows
          Opens kev:
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0
          Opens key:
                                                                                                                                                         HKLM\software\microsoft\windows
 nt \verb|\color= | ction| software protection platform \verb|\plugins| objects \verb|\msft:spp/volume/services/kms/activation info/1.0 | ction platform 
            Opens key:
                                                                                                                                                         HKLM\software\microsoft\windows
 nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft|: spp/windows functionality/agent/7.0| and the protection of the platform of
            Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
             Opens key:
                                                                                                                                                          HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
```

```
Opens key:
                               HKLM\software\microsoft\windows nt\currentversion\
  Opens key:
                               HKLM\system\setup\status
  Opens key:
                               HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\reboot.sl_brt_commit
  Opens key:
                               HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0
  Opens kev:
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 1237&subsys 00000000&rev 02\3&267a616a&1&00
  Opens kev:
Opens kev:
                               Opens key:
  Opens key:
                               Opens key:
                               Opens key:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0
  Opens kev:
                               HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0
  Opens key
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09
                               HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0
  Opens kev:
  Opens key:
                                                                                                         _1.0.7.3_\5&34baf594&0&0.0.0
HKLM\system\currentcontrolset\enum\ide\diskhitachi
                               HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1
  Opens key:
  Opens key:
HKLM \ system \ current control set \ enum \ pci \ ven\_80ee \ dev\_beef \ subsys\_00000000 \ rev\_00 \ 3\&267a616a\&1\&10 \ reversible \ for the property of the p
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34\
  Opens key:
                               HKLM\system\wpa\
  Opens key:
                               HKLM\system\wpa\478c035f-04bc-48c7-b324-2462d786dad7-5p-9\
  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\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14\
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15\
  Opens kev:
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17\
  Opens key:
                               \label{localization} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18\label{localization}
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21\
  Opens key:
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23\
                               HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-24\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25\
  Opens kev:
                               HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-26\
  Opens key:
  Opens kev:
                               HKLM\svstem\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28\
  Opens key:
                               Opens key:
                               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:
                               HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-33\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4\
  Opens key:
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5\
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6\
  Opens key:
  Opens key:
                               HKI M\svstem\wna\8dec0af1-0341-4h93-85cd-72606c2df94c-6n-7\
  Opens key:
                               HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-8\
  Opens key:
                               \label{local-eq:hklm} $$HKLM \simeq \ensuremath{\mbox{Wpa}\ensuremath{\mbox{8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9}$} $$
  Opens key:
                               0040963251e5}
  Opens key:
                               Opens key:
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
  Opens key:
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\treatas
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32
  Opens key:
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:
  Opens key:
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:
                               HKLM\software\microsoft\msxm160
  Opens kev:
                               HKLM\software\microsoft\windowsruntime\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}
                               Opens key:
  Opens kev:
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
  Opens key:
                               HKCR \clsid \ \ \{88d96a08-f192-11d4-a65f-0040963251e5\} \ \ treat as
  Opens key:
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32
  Opens key:
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler
                               HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-
  Opens key:
73e6154572dd}
  Opens key:
                               HKCR\activatableclasses\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
  Opens key:
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
  Opens key:
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32
  Opens key:
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32
  Opens key:
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler
  Opens key:
  Opens key:
                               {\tt HKLM \ } system \verb|\  current control set \verb|\  control \ | product options
  Opens key:
                               HKLM\system\currentcontrolset\services\wpdbusenum
  Opens key:
                               HKLM\system\currentcontrolset\services\wpdbusenum\parameters
```

 $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + action$

Opens key:

```
center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
                                                                            323e85a1ce84}
     Opens key:
                                                                            HKCR \ activatable classes \ \ clsid \ \ \{9 dac 2 c1 e-7 c5 c-40 eb-833 b-323 e85 a1 ce84\}
     Opens key:
                                                                            HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
                                                                            HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
     Opens kev:
     Opens key:
                                                                            HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\treatas
                                                                            HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
     Opens key:
    Opens key
                                                                            HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32
     Opens key:
                                                                            HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\
     Opens key:
                                                                            HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprochandler32
                                                                            HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
     Opens key:
                                                                            HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
     Opens key
323e85a1ce84}\inprochandler
    Opens key:
                                                                            HKCR\clsid\{9} dac2c1e-7c5c-40eb-833b-323e85a1ce84\}\inprochandler
                                                                            HKLM\software\microsoft\security center
    Opens key:
    Opens kev:
                                                                            HKLM\software\policies\microsoft\internet explorer\security
    Opens key:
                                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
    Opens key:
                                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
    Opens key:
                                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
    Opens key:
                                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
    Opens key:
                                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zones\0
    Opens kev:
                                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
    Opens kev:
                                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
     Opens key:
                                                                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                                                            \label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\notation{ Internet of the properties of the 
     Opens key:
 settings\zones\4
     Opens key:
                                                                            HKCU\software\policies\microsoft\internet explorer
     Opens key:
                                                                            HKCU\software\microsoft\internet explorer\security
    Opens key:
                                                                            HKLM\software\microsoft\internet explorer\security
     Opens kev:
                                                                            HKCU\software\microsoft\windows\currentversion\internet settings\zones
    Opens key:
                                                                            HKLM\software\microsoft\windows\currentyersion\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:
                                                                            {\it HKLM} \verb|\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 \ activatable classes \ \ clsid \ \ \ \{ca236752-2e77-4386-b63b-0e34774a413d\}
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
     Opens kev:
    Opens key:
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
    Opens key
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\treatas
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
     Opens key:
     Opens key
                                                                           HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32
     Opens key:
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
     Opens key:
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler32
                                                                            HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
      Opens key:
                                                                            HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
     Opens key
0e34774a413d}\inprochandler
    Opens key:
                                                                           HKCR \ clsid \ \{ca236752-2e77-4386-b63b-0e34774a413d\} \ in prochandler
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows\windows error reporting
    Opens key:
                                                                            HKCU\software\policies\microsoft\windows\windows error reporting
     Opens key:
                                                                            HKCU\software\microsoft\windows\windows error reporting
    Opens key:
                                                                            HKLM\software\microsoft\windows\windows error reporting\syspreplock
    Opens key:
                                                                            HKCU\software\microsoft\windows\windows error reporting\erc
    Opens key:
                                                                            HKCU \ software \ \verb|microsoft| windows \ \verb|current| version \ \verb|explorer| session in follows \ \verb|current| session in follows \ \verb|explorer| session in follows \ \ explorer| ses
    Opens key:
\label{thm:local_hammon} HKCU \software \microsoft \windows \current version \explorer \session in folders \current version \current \cu
      Opens key:
                                                                            HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{88d96a05 - f192 - 11d4 - a65f - f192 - f1
0040963251e5}
                                                                            HKCR\activatableclasses\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
     Opens key:
     Opens key:
                                                                            HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
     Opens key:
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
     Opens key:
                                                                            HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\treatas
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
     Opens key:
                                                                           HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
    Opens kev:
0040963251e5}\inprocserver32
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
     Opens key:
     Opens key:
                                                                            HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprochandler32
      Opens key:
                                                                            HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
     Opens key:
                                                                            HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
```

```
0040963251e5}\inprochandler
                         HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:
                         HKLM\software\microsoft\windows\currentversion\action
 Opens key
center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
```

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3be-belle + belle + belle$

499afcec98c4}

Opens key: HKCR\activatableclasses\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4} HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4} Opens key:

HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4} Opens key: Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-

499afcec98c4}\treatas

Opens key: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas Opens key: HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-

499afcec98c4}\inprocserver32

HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-Opens key

499afcec98c4}\inprochandler32

Opens key: $HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\ \ in prochandler 32$

HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-Opens key:

499afcec98c4}\inprochandler

HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler Opens key:

 ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action}$ Opens key:

center\providers\com\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}

Opens key:

f0aa6db5d4bc}

Opens key: HKCR\activatableclasses\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc} Opens key: HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}

Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc} HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-Opens key:

f0aa6db5d4bc}\treatas

Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-Opens key:

f0aa6db5d4bc}\inprocserver32

HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-Opens kev:

f0aa6db5d4bc}\inprochandler32

Opens key: $HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\label{line} In prochamble r32$

Opens key HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-

f0aa6db5d4bc}\inprochandler

Opens key: HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler Opens key: HKLM\software\microsoft\windows\currentversion\explorer Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash windows \backslash current version \backslash action}$

center\providers\com\{d26de5c1-c061-43f7-9c40-7517526cf1c1}

 $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-d3f7-9c40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-c061-d3f7-gc40-d26de5c1-d$ Opens kev:

7517526cf1c13

HKCR\activatableclasses\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1} Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1} Opens key: $HKCR \ clsid \ \{d26de5c1-c061-43f7-9c40-7517526cf1c1\}$ Opens kev:

HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-

Opens key: 7517526cf1c1}\treatas

 $HKCR \ clsid \ \{d26de5c1-c061-43f7-9c40-7517526cf1c1\} \ treat as$ Opens key: Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-

7517526cf1c1}\inprocserver32

HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-

7517526cf1c1}\inprochandler32

HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler32 Opens kev:

HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-Opens key:

7517526cf1c1}\inprochandler

 $HKCR\clsid\d26de5c1-c061-43f7-9c40-7517526cf1c1\$ \inprochandler Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\startupnotify Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action}$

center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}

 $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{6ae07dc1-0244-4c6f-9ab0-144$ Opens key

5017a56357c3}

 $HKCR \ activatable classes \ \ clsid \ \ \{6ae07dc1-0244-4c6f-9ab0-5017a56357c3\}$ Opens key: HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} Opens key:

Opens key: HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-Opens kev:

5017a56357c3}

HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3} Opens key:

Opens key $HKCU \setminus software \setminus classes \setminus activatable classes \setminus clsid \setminus \{6ae07dc1-0244-4c6f-9ab0-1$

5017a56357c3}

Opens key: ${\it HKLM} \verb|\software\microsoft\windows\currentversion\action$

center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}

Opens key:

40cd513679d5}

HKCR\activatableclasses\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5} Opens kev: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5} Opens key:

Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5} HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-Opens key

40cd513679d5}\treatas

HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-Opens kev:

40cd513679d5}\inprocserver32

 $HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\ \ \ inprocserver 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-

40cd513679d5}\inprochandler32

Opens key: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32

HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-Opens key:

40cd513679d5}\inprochandler HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-Opens key windowsbackup/actioncenter Opens key: $HKLM \software \mbox{\tt microsoft-windows-current} version \mbox{\tt winevt\channels\mbox{\tt microsoft-windows-current}} \\$ windowsbackup/actioncenter HKLM\software\microsoft\windows\currentversion\action Opens kev: $center \verb|\providers| eventlog \verb|\dab69a6a-4d2a-4d44-94bf-e0091898c881|$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsnetworkaccessprotection/whc Opens key: $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$w$indows$} - \mbox{winevt$} \channels \mbox{$\mbox{windows$} - \mbox{$w$inevt$} \channels \mbox{$\mbox{$w$indows$} - \mbox{winevt$} \channels \mbox{$\mbox{winevt$} - \mbox{$w$inevt$} \channels \mbox{$\mbox{$w$inevt$} - \mbox{winevt$} \channels \mbox{$\mbox{winevt$} - \mbox{$\mbox{winevt$} - \mbox{$w$inevt$} \channels \mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$\mbox{winevt$} - \mbox{$\mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$\mbox{winevt$} - \mbox{$\mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$\mbox{winevt$} - \mbox{$\mbox{\mb networkaccessprotection/who HKLM\software\microsoft\windows\currentversion\action Opens key: center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78} Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowswindows defender/whc Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-windows defender/whc Opens key: HKLM\software\microsoft\windows\currentversion\action $center \verb|\providers| eventlog \verb|\{a5268b8e-7db5-465b-bab7-bdcda39a394a\}|$ $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ event \+ log \+ microsoft - windows - log \+ microsoft - w$ Opens key: diagnosis-scheduled/operational Opens key: $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -diagnosis-diagnosi$ scheduled/operational Opens key: ${\it HKLM} \verb|\software\microsoft\windows\currentversion\action$ center\providers\eventlog\{de7b24ea-73c8-4a09-985d-5bdadcfa9017} Opens kev: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowstaskscheduler/maintenance Opens kev: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowstaskscheduler/maintenance HKLM\software\microsoft\windows\currentversion\action Opens key: $center \verb|\providers| eventlog \verb|\f134ea407-755d-4a93-b8a6-f290cd155023| \}$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowshomegroup control panel/operational Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-homegroup control panel/operational Opens key: HKLM\software\microsoft\windows\currentversion\action $center \providers \eventlog \end{c4efc9bb-2570-4821-8923-1bad317d2d4b}$ HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-Opens key: security-spp-ux-notifications/actioncenter Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-uxnotifications/actioncenter Opens key: ${\it HKLM} \verb|\software\microsoft\windows\currentversion\action$ $center \providers \eventlog \b447b4db-7780-11e0-ada3-18a90531a85a\}$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsfilehistory-core/whc Opens kev: core/whc HKLM\software\microsoft\windows\currentversion\action Opens kev: $center \verb|\providers| eventlog \verb|\f37a1c-a68d-4d6e-8c9b-f79e8b16c482| \\$ Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windowsntfs/whc Opens key: $HKLM \ software \ microsoft\ windows \ - trentversion \ winevt \ channels \ microsoft\ - windows \ - tfs/whc$ ${\it HKLM} \verb|\software\microsoft\windows\currentversion\action$ $center \verb|\providers| \{2374911b-b114-42fe-900d-54f95fee92e5\}|$ HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-shell-Opens key: connectedaccountstate/actioncenter Opens key: $HKLM \ software \ microsoft\ windows\ - shell-like \ microsoft\ - windows\ - shell-like \ microsoft\ - windows\ - shell-like \ microsoft\ - windows\ - shell-like \ - windows\ - wi$ connectedaccountstate/actioncenter HKLM\software\microsoft\windows\currentversion\action Opens key: Opens key: $\label{local-control} \mbox{HKLM} \mbox{$\tt NSYSTEM} \mbox{$\tt Current control set} \mbox{$\tt Services} \mbox{$\tt NSYSTEM} \mbox{$\tt NSYSTEM}$ userpnp/actioncenter Opens key: $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$w$indows$} - \mbox{winevt$} \channels \mbox{$\mbox{windows$} - \mbox{$w$inevt$} \channels \mbox{$\mbox{$w$indows$} - \mbox{winevt$} \channels \mbox{$\mbox{winevt$} - \mbox{$w$inevt$} \channels \mbox{$\mbox{$w$inevt$} - \mbox{winevt$} \channels \mbox{$\mbox{winevt$} - \mbox{$\mbox{winevt$} - \mbox{$w$inevt$} \channels \mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$\mbox{winevt$} - \mbox{$\mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$\mbox{winevt$} - \mbox{$\mbox{$\mbox{$w$inevt$} - \mbox{$\mbox{$\mbox{winevt$} - \mbox{$\mbox{\mb userpnp/actioncenter Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action}$ $center \verb|\providers| \{aa4c798d-d91b-4b07-a013-787f5803d6fc\}|$ 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

 $Queries\ value: \\ HKLM\software\mbox{\mbox{microsoft\windows\currentversion\sidebyside[preferexternalmanifest]}}$

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers [transparentenabled]|$

HKCU\control panel\desktop[preferreduilanguages]

HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value:

Queries value:

Oueries value:

```
Queries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
                         HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
                         HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Oueries value:
                         {\it HKLM} \verb|\software\microsoft| ole[pageallocatorsystem heapisprivate]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\ole[aggressivemtatesting]
 Oueries value:
                         HKCU\console[screencolors]
 Queries value:
                         HKCU\console[popupcolors]
 Queries value:
                         HKCU\console[insertmode]
                         HKCU\console[quickedit]
  Queries value:
                         HKCU\console[codepage]
  Oueries value:
                         HKCU\console[screenbuffersize]
 Queries value:
 Queries value:
                         HKCU\console[windowsize]
                         HKCU\console[windowposition]
 Queries value:
 Oueries value:
                         HKCU\console[fontsize]
 Oueries value:
                         HKCU\console[fontfamily]
 Queries value:
                         HKCU\console[fontweight]
 Oueries value:
                         HKCU\console[facename]
 Queries value:
                         HKCU\console[cursorsize]
 Oueries value:
                         HKCU\console[historybuffersize]
                         HKCU\console[numberofhistorybuffers]
  Queries value:
 Queries value:
                         HKCU\console[historynodup]
  Queries value:
                         HKCU\console[colortable00]
  Oueries value:
                         HKCU\console[colortable01]
 Queries value:
                         HKCU\console[colortable02]
                         HKCU\console[colortable03]
 Oueries value:
 Queries value:
                         HKCU\console[colortable04]
 Oueries value:
                         HKCU\console[colortable051
 Oueries value:
                         HKCU\console[colortable061
                         HKCU\console[colortable071
 Oueries value:
 Queries value:
                         HKCU\console[colortable08]
 Oueries value:
                         HKCU\console[colortable09]
 Queries value:
                         HKCU\console[colortable10]
                         HKCU\console[colortable11]
  Queries value:
                         HKCU\console[colortable12]
  Oueries value:
 Queries value:
                         HKCU\console[colortable13]
 Queries value:
                         HKCU\console[colortable14]
 Queries value:
                         HKCU\console[colortable15]
 Oueries value:
                         HKCU\console[loadconime]
                         HKCU\console[extendededitkev]
 Oueries value:
 Oueries value:
                         HKCU\console[extendededitkeycustom]
                         HKCU\console[worddelimiters]
 Oueries value:
 Oueries value:
                         HKCU\console[trimleadingzeros]
 Oueries value:
                         HKCU\console[enablecolorselection]
 Oueries value:
                         HKCU\console[scrollscale]
 Queries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
 Queries value:
                         HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                         HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Oueries value:
                         HKLM\svstem\currentcontrolset\control\nls\locale[00000409]
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
 Queries value:
                         HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Oueries value:
                         \label{lem:hklmsoftware} \verb+windows \windows error reporting \verb+wmr[disable]+ \\
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Oueries value:
                         HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
                         HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:
  Queries value:
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]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Oueries value:
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Oueries value:
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:
HKCU\software\microsoft\windows
  Queries value:
nt\currentversion\appcompatflags[showdebuginfo]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Queries value:
options\dllnxoptions[toggleservice32.exe]
 Oueries value:
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
```

HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Oueries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

Oueries value: HKLM\software\microsoft\rpc[idletimerwindow]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Queries value: HKLM\software\microsoft\com3[com+enabled]

```
Oueries value:
                           HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
                           HKLM\software\microsoft\windows nt\currentversion\compatibility32[alg]
  Queries value:
                           HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
 Queries value:
                           HKLM\software\microsoft\ole[defaultaccesspermission]
                           HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
 Oueries value:
 Oueries value:
                           HKLM \ \ software \ \ \ \ trong \ \ \ \ trong
cryptographic provider[type]
                           . HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 Queries value:
cryptographic provider[image path]
                           \hbox{\tt HKLM} : software \verb|\policies| microsoft| cryptography[privkeycachemaxitems]
  Queries value:
 Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:
                           HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                           HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
                           HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
  Oueries value:
 Queries value:
                           HKLM\software\microsoft\rpc\extensions[ndroleextdll]
 Queries value:
                           HKLM\software\microsoft\ole[maxsxshashcount]
                           HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_misc]
 Oueries value:
 Oueries value:
                           {\tt HKLM \setminus software \setminus microsoft \setminus msdtc \setminus tracing \setminus sources[trace\_cm]}
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
 Oueries value:
                           \label{lem:hklm} \verb+ Kklm \ software \ \verb+ microsoft \ \verb+ msdtc \ \verb+ tracing \ \verb+ sources [trace\_svc] \\
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_gateway]
 Oueries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_ui]
  Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_contact]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
  Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_cluster]
  Oueries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_resource]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_tip]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_log]
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
 Oueries value:
 Oueries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_ktmrm]
 Oueries value:
                           \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ msdtc\+ tracing\+ sources[trace\_vssbackup]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon]
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_tm]
  Queries value:
  Oueries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\sources[trace_wmi]
  Queries value:
                           HKLM\software\microsoft\msdtc\tracing\output[tracefilepath]
 Queries value:
                           HKLM\software\microsoft\msdtc\tracing\output[memorybuffersize]
                           HKLM\software\microsoft\msdtc\tracing\output[debugoutenabled]
 Oueries value:
                           HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\tracing\msdtc\misc[disabletracing]
                           HKLM \setminus software \setminus microsoft \setminus msdtc[noparallellogflushnotification] \\
  Queries value:
 Oueries value:
\label{lem:hklm} \verb+KLM\+ software \verb+\microsoft\+ msdtc[snapshotprefer transaction stime outduring backup]
  Oueries value:
                           HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
 Queries value:
                           HKLM \setminus software \setminus microsoft \setminus msdtc [disable termination on heap corruption] \\
  Queries value:
                           HKLM\software\microsoft\msdtc[sysprepinprogress]
 Queries value:
                           HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\description[]
  Oueries value:
 Queries value:
                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\svcid[]
                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\host[]
 Queries value:
                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\clsid[]
 Oueries value:
                           HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
 Oueries value:
 Oueries value:
                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol[]
                           HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint[]
 Queries value:
 Oueries value:
                           HKCR\cid.local\15546232-d044-45d4-88a8-
Ob84583f2fe1\customproperties\log\size[]
  Oueries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oraclexalibpath]
  Queries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oraclesqllibpath]
  Queries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oracleocilibpath]
  Queries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
 Oueries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib]
 Oueries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
 Queries value:
                           HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
 Queries value:
                           HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
                           HKLM\software\microsoft\msdtc\security[accountname]
 Oueries value:
                           HKLM\software\microsoft\msdtc\security[networkdtcaccess]
 Oueries value:
 Oueries value:
                           HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
 Oueries value:
                           HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
 Queries value:
                           HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
  Queries value:
                           HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
                           HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
  Queries value:
                           HKLM\software\microsoft\msdtc\security[xatransactions]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\msdtc\security[lutransactions]
                           HKCR\cid.local\15546232-d044-45d4-88a8-
 Queries value:
0b84583f2fe1\customproperties\log\path[]
                           HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-
 Oueries value:
8bd7-da8f1a74051a]
                           HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\tracing\msdtc\loggingoptions[requests ession up]|
 Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[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]
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxfilesize]
                                   HKLM\system\currentcontrolset\control\timezoneinformation[bias]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\timezoneinformation[standardname]
  Queries value:
                                   HKLM\system\currentcontrolset\control\timezoneinformation[standardbias]
                                   HKLM\system\currentcontrolset\control\timezoneinformation[standardstart]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[uniqueid]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[active]
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[level]
  Queries value:
                                  HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[controlflags]
                                  HKLM\software\microsoft\windows
  Queries value:
\verb| nt\currentversion \rangle is defined as the constant of the con
                                  HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
  Queries value:
                                   HKLM\system\currentcontrolset\control\wmi\security[e80aa9fe-913d-4ede-
af58-73e332dcac8d1
  Oueries value:
                                   HKLM\software\microsoft\msdtc[dtcmaxsessions]
  Queries value:
                                   HKLM\software\microsoft\msdtc[donotgoidle]
  Queries value:
                                   HKLM\software\microsoft\msdtc[disabletippassthrucheck]
                                   HKLM\software\microsoft\msdtc[mincheckpointinterval]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc[maxcheckpointinterval]
                                   HKLM\software\microsoft\msdtc[waitforallxabranchprepares]
  Oueries value:
                                   HKLM\software\microsoft\msdtc\security[snapshotsecuritydisabled]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc[servertcpport]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion[currentversion]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[cmcancelrpcafter]
                                   HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc[cmmaxidlepings]
  Queries value:
                                   HKLM\software\microsoft\msdtc[cmpingfreqsecs]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[cmverbose]
  Queries value:
                                   HKLM\software\microsoft\msdtc[rpcqoscapabilities]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[rpcgosidentitv]
                                   HKLM\software\microsoft\msdtc[rpcauthnsvc]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\msdtc[numcccimhistoryentries]
                                   HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\description[]
  Oueries value:
                                   HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\svcid[]
  Oueries value:
  Oueries value:
                                   HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host[]
  Oueries value:
                                   HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid[]
  Queries value:
                                   HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
  Queries value:
                                   HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\protocol[]
  Queries value:
                                   HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint[]
  Oueries value:
                                   HKCU\control panel\international[scurrencyoverride]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
                                   HKLM\software\microsoft\msdtc[notracking]
  Oueries value:
                                   HKLM\software\microsoft\rpc\securityservice[9]
  Oueries value:
  Oueries value:
HKLM \setminus system \setminus current control \setminus security providers [security providers]
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\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:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Queries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Queries value:
                                   HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc\description[]
                                   HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\description[]
  Oueries value:
  Oueries value:
                                   HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid[]
  Oueries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus access providers [martaextension]
  Queries value:
                                   HKLM\software\microsoft\msdtc[shared_memory_mutex_timeout]
  Queries value:
                                   HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host[]
                                   HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid[]
  Queries value:
                                   HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
  Oueries value:
  Queries value:
                                   HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol[]
  Queries value:
                                   HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\endpoint[]
                                   HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
  Queries value:
                                   HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[transactionbridge]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[logwarnenabled]
  Oueries value:
                                   HKLM\software\microsoft\msdtc[suppressduplicateduration]
  Queries value:
                                   HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
  Oueries value:
  Queries value:
                                   HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
                                   HKCR\clsid\{304ce942-6e39-40d8-943a-
  Queries value:
```

b913c40c9cd4}\inprocserver32[threadingmodel]

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

Queries value: HKLM\software\microsoft\msdtc[supportns]

Queries value:

Oueries value:

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

Queries value:

 $\label{thm:loss-twindows-universion-winevt-channels-microsoft-windows-appx deployments erver/operational [enabled] \\$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-appx deployments erver/operational [file max]$

Queries value

 $\label{thm:loss-twindows} HKLM \software \microsoft-windows-appx deployments erver/operational [file counter]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:loss-twindows-universion-winevt-channels-microsoft-windows-appx deployments erver/operational [latency] \\$

Queries value:

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

Oueries value:

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

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \microsoft \windows \software \microsoft \windows \appx deployments erver/operational [level]$

Queries value:

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

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \solutions \microsoft \-windows \-appx deployments \-error \-perational \max \-size]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -appx deployments erver/operational \ [max size upper]$

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows \label{lem:hklm} appx deployments erver/operational [autobackuplogfiles]$

Queries value:

 $HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} where \label{lem:hklm} winevt \label{lem:hklm} where \label{lem:hklm} where \label{lem:hklm} hklm \label{lem:hklm} where \label{lem:hklm} hkllm \label{lem:hklm} where \label{lem:hklm} hkllm \label{lem:hklm} where \label{lem:hkllm} hkllm \label{lkllm} hkllm \label{lkllm} hkllm \label{lkllm} hkllm$

Queries value:

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

Queries value:

 $\label{thm:hklm:software:microsoft-windows-unrentversion-winevt-channels-microsoft-windows-appx deployments erver/operational [isolation]$

Queries value:

 $\label{thm:hammon} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows-appxdeploymentserver/operational[owningpublisher]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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[latency]

Queries value:

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

Oueries value:

 $\label{thm:hammels} HKLM\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-networkprofile/operational[sidtype]$

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

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

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:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - network profile/operational[file]$

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \scalebox{\sim kernel-storemgr/operational[type]} \\$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_hammels_microsoft_windows_kernelstoremgr/operational[filecounter]} HKLM \software \mbox{\sc microsoft-windows-kernel-storemgr/operational[filecounter]}$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-kernel-storem \gr/operational \[buffer \size]$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-kernel-storem \scalebox{\color=loss} winevt\channels \microsoft-windows-kernel-storem \scalebox{\color=loss} winevt\channel\scalebox{\color=loss} wi$

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:

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

Queries value:

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

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-kernel-storem \grapher \grapher$

Queries value:

 $\label{thm:local-problem} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-kernel-storem \graph{graph}{graph} \scalebox{0.05\columnwidth}{graph} \scalebox{0.05\columnwidth}{graph}$

Queries value:

 $\label{thm:local_maxsize} HKLM \software \microsoft-windows-kernel-storem \scalebox{\colorable}{rho} winevt \channels \microsoft-windows-kernel-storem \scalebox{\colorable}{rho} \sc$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-kernel-storem \scalebox{\scalebox$

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - kernel-part \ windows \ - kernel-part \ - kernel-part$ 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-leave \ microsoft \ - windows \ - kernel-leave \$ 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:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} windows \end{tabular} consoft \end{tabular} windows \end{tabular} and \end{tabular} windows \end{tabular} and \end{tabular} windows \end{tabular} and \end{tabular} windows \end{tabular} and \end{tabular} windows \end{tabular} windows$ 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]

Queries 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:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc} windows \screen \screen_hammon_ha$

Oueries value

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} which are \label{lem:hklm} which is a simple constant of the lemma support of the lemma$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-problem} HKLM \software \mbox{$\$

Queries value:

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

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:

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

Queries value:

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

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:

 $\label{thm:hklm} HKLM \noindent \n$

Queries value:

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

Queries value: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\compatibility32[ui0detect]|\\$

Queries value: HKU\.default\control panel\desktop[preferreduilanguages]

Queries value: HKU\.default\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{$154849625-5478-4994-a5ba-3e3b0328c30d} \ [message filename]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\mbox{$154849625-5478-4994-a5ba-3e3b0328c30d}[categorymessagefile]} \\$

Queries value:

Oueries value:

 $HKLM \label{likelihood} HKLM \label{likelihoodd} HKLM \labe$

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{\mb

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{$1-a6d7-4695-8e1e-26931d2012f4} [category message file]$

Queries value:

```
26931d2012f4}[resourcefilename]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e
26931d2012f4}[parameterfilename]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e
26931d2012f4}[helplink]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-
26931d2012f4}[enabled]
   Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{555908d1-a6d7-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e1e-4695-8e
26931d2012f4}[categorycount]
   Queries value:
26931d2012f4}\channelreferences[count]
   Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-
26931d2012f4}\channelreferences\0[1
   Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-
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\software\microsoft\windows
nt\currentversion\svchost[localservicepeernet]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile[svchost]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus p2pimsvc \setminus parameters [service manifest]
   Queries value:
                                              HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
                                               HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
   Queries value:
   Oueries value:
                                               HKLM\software\policies\microsoft\peernet[disabled]
   Queries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedllunloadonstop]
   Queries value:
                                              HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll]
   Oueries value:
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]
   Oueries value:
                                               HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
   Queries value:
                                               HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
   Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[next catalog entry id]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries64]
   Oueries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\000000000006fpackedcatalogitem1
   Queries value:
Oueries value:
Oueries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ [num\_catalog\_entries 64]
   Oueries value:
Oueries value:
Oueries value:
Queries value:
HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ namespace\_catalog5 \ \ catalog\_entries 64 \ \ 000000000001 \ [address family]
```

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[enabled]
 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\000000000001[providerinfo]
 Oueries value:
- $\label{lem:hklm/system/current} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000002[librarypath]\ Queries\value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries 64 \ 0000000000002 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000002[providerid] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000002[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[enabled]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries 64 \000000000002 \[version] \queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[storesserviceclassinfo]
 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[addressfamily] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries 64 \0000000000003 \[supported names pace_value:] \\$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries 64 \ 0000000000003 \ [providerinfo] \ Queries \ value:$
- $\label{lem:hklm/system/current} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries 64 \namespace \namespace_catalog 5 \catalog_entries 64 \namespace \namespace_catalog 5 \catalog_entries 64 \namespace_catalog 5 \namespace_ca$
- $\label{lem:hklmsystem} HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000004 \ [providerid] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[addressfamily]
 Queries value:
- 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[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[storesserviceclassinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries 64 \ 0000000000004 \ [providerinfo] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
 Oueries value:
- $\label{lem:hammaspace_catalogs} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries 64 \0000000000005 \[displaystring]\queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[supportednamespace]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries 64 \000000000005 \cite{lemonths} enabled] Queries value:$
- KKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000005[version]
 Oueries 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[displaystring] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 0000000000006 \ [address family] \ Queries \ value:$

```
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\000000000006[version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\00000000006[storesserviceclassinfo]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerinfo]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:
                                            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
                                            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                                           HKLM\system\currentcontrolset\services\winsock\setup
  Queries value:
migration\providers\tcpip6[winsock 2.0 provider id]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [maxsock addrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
  Oueries value:
55779daa70e9}[domain]
   Queries value:
55779daa70e9}[dhcpdomain]
  Queries value:
HKLM \ system \ current controls et \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-805d63-805d63-805d63-805d63-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d648-805d648-805d648-805d64-805d648-805d648-805d648-805d64-805d648-805d648-805d648-805d648-805d64
55779daa70e9}[dhcpv6domain]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
   Oueries value:
806e6f6e6963}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
                                            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
  Oueries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
   Oueries value:
                                           HKLM\software\microsoft\samclient[machineid]
   Queries value:
                                           HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[seedserver]
   Queries value:
                                           HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastpublish]
                                           HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastsearch]
   Queries value:
                                           HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disabled]
                                           HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
   Queries value:
linklocal\linklocal_ff00::%12/8[searchonly]
                                           Queries value:
linklocal\linklocal ff00::%12/8[mincpalifetime]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
   Queries value:
                                           HKLM \  \  \, in the constraint of the constrai
19[profileimagepath]
   Queries value:
                                            HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
   Queries value:
                                            HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
                                            HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
   Queries value:
  Queries value:
                                            HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ rsa
schannel cryptographic provider[type]
```

 $HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ rsa$

HKLM\software\policies\microsoft\cryptography[forcekeyprotection]

 ${\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}$ 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name] Queries value:

 ${\it HKLM} \backslash {\it software} \backslash {\it microsoft} \backslash {\it windows}$

schannel cryptographic provider[image path]

nt\currentversion\profilelist[programdata]

Oueries value:

Queries value:

Queries value:

Oueries value:

```
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
                                   HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
  Queries value:
                                   {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7[name]
                                   HKLM\software\microsoft\cryptography\oid\encodingtype
  Oueries value:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7[name]
                                   {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
  Oueries value:
{\tt 0} \verb| cryptdllfindoidinfo \verb| 1.3.6.1.4.1.311.76.6.1!7[name] \\
  Oueries value:
Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[usefilter]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[disableheaplookaside]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[frontendheapdebugoptions]
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value:
options\spoolsv.exe[shutdownflags]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[unloadeventtracedepth]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[tracingflags]
  Queries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\spoolsv.exe[minimumstackcommitinbytes]
                                   \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} AKLM \end{tabular} \begin{tabular}{ll} AKL
  Queries value:
options\spoolsv.exe[breakoninitializeprocessfailure]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[keepactivationcontextsalive]
  Queries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[trackactivationcontextreleases]
                                   \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
  Queries value:
options\spoolsv.exe[maxdeadactivationcontexts]
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
  Oueries value:
options\spoolsv.exe[globalflag]
  Queries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\spoolsv.exe[cwdillegalindllsearch]
  Queries value:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\spoolsv.exe[debugprocessheaponly]
  Oueries value:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spoolsv.exe[searchpathmode]
                                   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[spoolsv]
                                   HKLM\system\currentcontrolset\control\wmi\securitv[d2e1bab2-eb9b-4ba7-
  Oueries value:
9123-19c01ddc4f781
  Oueries value:
                                   HKLM\system\currentcontrolset\control\wmi\security[c9bf4a9e-d547-4d11-
8242-e03a18b5be011
  Oueries value:
                                   \label{lem:hklm} \verb+Kklm \ system \ current control \ \ print [exception handler enabled]
  Queries value:
                                   HKLM\system\currentcontrolset\control\wmi\security[b1ad9b49-051a-4896-
ae24-ebc9b8676e761
  Queries value:
                                   {\tt HKLM \ } system \verb| current control \verb| set \verb| control \verb| print[thread notify max]|
  Queries value:
                                   HKLM\system\currentcontrolset\control\print[threadnotifyidlelife]
  Queries value:
                                   HKLM\system\currentcontrolset\control\print[threadnotifysleep]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\print[maxrpcsize]
                                   HKLM\system\currentcontrolset\control\print[maxrpccalls]
  Oueries value:
                                   HKLM\software\microsoft\sqmclient\windows\disabledprocesses[71e8376c]
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\sqmclient\windows[studyid]
                                   HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
  Oueries value:
  Oueries value:
                                   {\tt HKLM \ } system \verb|\ current control \ | \ print[call exit process on shut down]
  Queries value:
HKLM \verb|\system| current controlset \verb|\services| lmhosts \verb|\parameters[enable user mode]|
  Queries value:
                                   8395-a606df8ef115]
                                   Queries value:
a369-f1759feedeb3]
  Queries value:
                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32 [vssvc]
  Oueries value:
                                   HKLM\software\microsoft\com3[finalizeractivitybypass]
  Queries value:
                                   HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
                                   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[]
                                   HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
  Queries value:
  Queries value:
                                   HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}[]
  Queries value:
                                   HKCR\clsid\{4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[]
                                   HKCR\clsid\{4e14fba2-2e22-11d1-9964-
  Queries value:
00c04fbbb345}\inprocserver32[threadingmodel]
                                   HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                   Oueries value:
                                   HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[]
  Queries value:
  Oueries value:
                                   HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\nprocserver32[]
  Queries value:
                                   HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[threadingmodel]
```

```
Oueries value:
                                                                  HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
     Queries value:
                                                                  HKCR\interface\{00000100-0000-0000-0000-00000000046}\proxystubclsid32[]
                                                                  HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
     Queries value:
                                                                  HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
     Queries value:
    Queries value:
                                                                  HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocserver32[inprocserver32]
                                                                  HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
     Oueries value:
                                                                 HKCR\clsid\{7542e960-79c7-11d1-88f9-
     Oueries value:
0080c7d771bf}\inprocserver32[threadingmodel]
                                                                 HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
    Oueries value:
     Oueries value:
HKLM\system\currentcontrolset\services\eventlog\application\vss[providerguid]
                                                                  HKLM\software\microsoft\windows
     Queries value:
 nt\currentversion\windows[displayversion]
                                                                  HKCU\control panel\desktop[paintdesktopversion]
     Queries value:
HKLM\system\currentcontrolset\services\audiosrv\parameters[servicedllunloadonstop]
     Queries value:
                                                                 HKLM\software\microsoft\windows nt\currentversion\svchost[wersvcgroup]
     Queries value:
HKLM\software\microsoft\windows\currentversion\audio[enablecapturemonitor]
                                                                 HKU\.default\control panel\international[scurrencyoverride]
     Oueries value:
     Oueries value:
                                                                  HKLM\system\currentcontrolset\services\wersvc\parameters[servicedll]
     Oueries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicemanifest]
                                                                  HKLM\system\currentcontrolset\services\wersvc\parameters[servicemain]
     Queries value:
                                                                  HKLM\system\currentcontrolset\control\wmi\security[6851adeb-79da-4250-
     Queries value:
 a440-f1f52d28711d]
     Queries value:
                                                                  HKLM\software\microsoft\windows\windows error reporting[servicetimeout]
     Oueries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicedllunloadonstop]
                                                                  HKLM\software\microsoft\windows nt\currentversion\svchost[imgsvc]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\services\stisvc\parameters[servicedll]
     Queries value:
     Oueries value:
HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest]
                                                                  \label{lem:hklm} \verb+Kklm \system \current control set \services \stisvc \parameters [service main]
     Oueries value:
     Queries value:
\label{lem:hklmsystem} \verb| HKLM \rangle is the limit of the li
     Queries value:
                                                                  HKLM\system\currentcontrolset\control\stillimage\trace[maxfilesize]
 HKLM\system\currentcontrolset\control\stillimage\trace[defaulttraceflags]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracemask]
     Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracelevel]
    Oueries value:
 HKLM\system\currentcontrolset\control\stillimage\trace[defaultmaxtracearraysize]
     Oueries value:
HKLM \setminus system \setminus current control \setminus stillimage \setminus trace[defaultenable object tracking]
     Oueries value:
                                                                  HKLM\system\currentcontrolset\control\stillimage\trace[heapoptions]
     Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[traceflags]
     Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracemask]
 HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracelevel]
    Oueries value:
Oueries value:
 HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[enableobjecttracking]
     Oueries value:
HKLM \ system \ current control \ stillimage \ trace \ wiaservc. dll[heapoptions]
     Oueries value:
                                                                  HKLM\software\microsoft\rpc\securityservice[10]
     Queries value:
                                                                  HKCR \land appid \land \{a1f4e726-8cf1-11d1-bf92-0060081ed811\} [authenticationlevel]
     Oueries value:
                                                                  HKCR \land appid \land \{a1f4e726-8cf1-11d1-bf92-0060081ed811\} [access permission]
     Queries value:
                                                                  HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[]
                                                                  HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
     Queries value:
     Queries value:
                                                                  HKLM\software\microsoft\windows\currentversion[devicepath]
     Oueries value:
                                                                  HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}[]
     Queries value:
                                                                  HKLM\system\currentcontrolset\control\stillimage[deviceid]
     Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected[defaulthandler]
                                                                 HKLM\system\currentcontrolset\control\stillimage\events\connected[guid]
    Oueries value:
     Oueries value:
HKLM \ system \ current control \ stillimage \ events \ connected \ \{ee1ddf29-1c65-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5cc-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-1c64-4ea6-b5c-
6c15f82b5905}[name]
    Queries value:
HKLM \ system \ current control \ stillimage \ events \ connected \ \{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-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-b5c-1c65-4ea6-b5c
6c15f82b5905}[desc]
HKLM \ system \ current control \ stillimage \ events \ connected \ \{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-b5
6c15f82b5905}[icon]
    Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-
6c15f82b5905}[cmdline]
    Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[defaulthandler]
    Oueries value:
HKLM \setminus system \setminus current control \setminus stillimage \setminus events \setminus 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] 759eb35cdf9a}[desc1 Oueries value: 759eb35cdf9a}[icon] Oueries value: 759eb35cdf9a}[cmdline] Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage[defaulthandler] Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage[guid] 759eb35cdf9a}[name] Queries value: 759eb35cdf9a}[desc1 Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon] Oueries value: 759eb35cdf9a}[cmdline] Queries value: Queries value: HKLM\system\currentcontrolset\control\stillimage\events\printimage[guid] Oueries value: 759eb35cdf9a}[name1 Oueries value: 759eb35cdf9a}[desc] Queries value: 759eb35cdf9a}[icon] Oueries value: HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline] Queries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[defaulthandler] Oueries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[guid] Oueries value: 783ce7a92f22}[name] Queries value: 783ce7a92f22}[desc] Queries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[icon] Oueries value: 783ce7a92f22\[cmdline1 Oueries value: 759eb35cdf9a}[name] Oueries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc] Queries value: 759eb35cdf9a}[icon] Oueries value: 759eb35cdf9a}[cmdline] Queries value: 7105fd3b53b1}[name] Queries value: 7105fd3b53b1}[desc] Queries value: 7105fd3b53b1}[icon] Queries value: 7105fd3b53b1}[cmdline] Oueries value: $HKLM \ system \ current control \ stillimage \ events \ scan but ton \ \{ee1ddf29-1c65-4ea6-b5cc-1c65-4ea6-b5c-1c65-4ea6$ 6c15f82b5905}[name] Queries value: $HKLM \ system \ current control \ stillimage \ events \ scan but ton \ \{ee1ddf29-1c65-4ea6-b5cc-1c65-4ea6-b5c-1c65-4ea6$ 6c15f82b5905}[desc] Oueries value:

 $\label{limage-events-scan} HKLM \system \current control still image \events \scan button \ee 1 ddf 29-1 c65-4 ea6-b5 cc-1 ddf 29-1 c65-4 ea6-b5 ea6-b5 ea6-b5 ea6-b5 ea6-b$

6c15f82b5905}[icon]

```
Oueries 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}[cmdline]
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]
                                                        HKLM\system\currentcontrolset\services\nativewifip[imagepath]
    Oueries value:
    Oueries value:
                                                        HKLM\system\currentcontrolset\services\nativewifip[objectname]
    Oueries value:
                                                        HKLM\system\currentcontrolset\services\nativewifip[type]
    Queries value:
                                                        HKLM\system\currentcontrolset\services\nativewifip[pnpflags]
   Queries value:
                                                        HKLM\system\currentcontrolset\control\wmi\security[d905ac1c-65e7-4242-
99ea-fe66a8355df8]
    Oueries value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
   Queries value:
                                                        HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filtertype]
                                                        HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Oueries value:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterruntype]
                                                        HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Oueries value:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterclass]
                                                        Queries value:
08002be10318\} \\ \{e475cf9a-60cd-4439-a75f-0079ce0e18a1\} \\ \\ ndi[unbindonattach]
                                                        HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
    Queries value:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindondetach]
    Queries value:
                                                        HKLM\system\currentcontrolset\services\ndisuio[imagepath]
                                                        HKLM\system\currentcontrolset\services\ndisuio[objectname]
    Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\services\ndisuio[type]
   Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&1&18[driver]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Oueries value:
08002be10318}\0010\linkage[upperbind]
    Oueries value:
                                                        HKI M\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Oueries value:
08002be10318}\0007\linkage[upperbind]
    Queries value:
55779daa70e9}[searchlist]
                                                        HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
    Queries value:
    Oueries value:
                                                        HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage[upperbind]
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value:
08002be10318}\0006\linkage[upperbind]
    Oueries value:
                                                        HKLM\system\currentcontrolset\services\ndisuio[pnpflags]
   Oueries value:
                                                        HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-
aded-5304bf8f636d1
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\wmi\security[b3eee223-d0a9-40cd-
adfc-50f1888138ab1
    Oueries value:
                                                        HKLM\system\currentcontrolset\services\ndisuio[legacypause]
    Queries value:
HKLM \ system \ current controls et \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-74c6-4dc1-87b7-405d63-805d63-805d63-805d63-805d63-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d64-805d648-805d648-805d648-805d64-805d648-805d648-805d648-805d64-805d648-805d648-805d648-805d648-805d64
55779daa70e9}[nameserver]
                                                        HKLM\system\currentcontrolset\services\ndisuio[ndisbootstart]
    Queries value:
                                                        HKLM\system\currentcontrolset\services\wlansvc[imagepath]
    Oueries value:
                                                        HKLM\system\currentcontrolset\services\wlansvc[wow64]
    Oueries value:
                                                        HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value:
08002be10318}\0004\linkage[upperbind]
    Queries value:
                                                        HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000[driver]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[upperbind]
    Queries 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]
                                                       HKLM\system\currentcontrolset\services\wlansvc[objectname]
   Oueries value:
                                                        HKLM\system\currentcontrolset\services\wlansvc[requiredprivileges]
    Oueries value:
    Oueries value:
                                                        HKLM \ system \ current controls et \ enum \ root \ ms\_pptpminiport \ 0000 [driver]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage[upperbind]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus wlansvc \setminus parameters [serviced llunload on stop]
                                                        HKLM\system\currentcontrolset\enum\root\*isatap\0000[driver]
    Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage[upperbind]
    Queries value:
                                                        HKLM\system\currentcontrolset\enum\root\*teredo\0000[driver]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
    Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus faces \setminus \{97e1de57-d6fa-11e1-be62-faces\} \setminus \{97e1de57-d6fa-11e1-be62-fac
806e6f6e6963}[dhcpnameserver]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\wmi\security[981f2d81-b1f3-11d0-
```

```
0000-00000000000001
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
      Queries value:
08002be10318}\0012\linkage[upperbind]
      Queries value:
                                                                            HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
     Queries value:
 08002be10318}\0002\linkage[upperbind]
                                                                            HKLM\system\currentcontrolset\enum\root\ms sstpminiport\0000[driver]
     Oueries value:
     Oueries value:
                                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318\0001\linkage[upperbind]
     Oueries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 08002be10318}\0000[netcfginstanceid]
     Queries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[netcfginstanceid]
      Queries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[netcfginstanceid]
     Oueries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 08002be10318}\0003[netcfginstanceid]
                                                                            HKLM\system\currentcontrolset\control\wmi\security[981f2d80-b1f3-11d0-
     Queries value:
 8dd7-00c04fc3358c]
     Oueries value:
                                                                            HKLM\software\microsoft\wcmsvc[wlanminsignalstrength]
     Oueries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[netcfginstanceid]
     Oueries value:
                                                                            08002be10318}\0005[netcfginstanceid]
      Queries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[netcfginstanceid]
     Queries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 08002be10318}\0007[netcfginstanceid]
     Oueries value:
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008[netcfginstanceid]
                                                                            HKLM\software\microsoft\wcmsvc[wlanweaksignalmeasureinterval]
     Oueries value:
                                                                            HKLM\software\microsoft\wcmsvc[wlangoodsignalmeasureinterval]
     Queries value:
                                                                            Oueries value:
08002be10318}\0009[netcfginstanceid]
     Oueries value
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 08002be10318}\0010[netcfginstanceid]
      Queries value:
                                                                            08002be10318}\0010[characteristics]
      Queries value:
                                                                            08002be10318}\0011[netcfginstanceid]
                                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
     Queries value:
08002be10318}\0012[netcfginstanceid]
     Queries value:
                                                                            HKLM\system\currentcontrolset\control\wmi\security[082f46b6-01f6-4511-
9044-d83675f466371
     Oueries value:
HKLM\software\microsoft\wcmsvc\subscriptionmanager[servertimeretryperiod]
     Queries value:
                                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011[characteristics]
     Queries value:
                                                                           08002be10318}\0012[characteristics]
                                                                            HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}[]
      Queries value:
     Queries value:
                                                                            HKCR\clsid\{5b035261-40f9-11d1-aaec-
 00805fc1270e}\inprocserver32[inprocserver32]
     Queries value:
                                                                           HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[]
                                                                           HKCR\clsid\{5b035261-40f9-11d1-aaec-
     Oueries value:
00805fc1270e}\inprocserver32[threadingmodel]
                                                                           HKLM\system\currentcontrolset\control\wmi\security[b6c2b638-4f86-4095-
     Oueries value:
 9446-dfc044e0663a1
     Oueries value:
                                                                            HKLM\system\currentcontrolset\control\wmi\security[41e8e8f3-7b6d-488e-
b350-f696dd24afb61
      Oueries value:
                                                                            {\tt HKLM \ } system \verb|\ current control \verb|\ control \verb|\ network[config]|
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{67d07935-283a-4791-8f8d-1864-1864, \ name \ name\ name \ 
 fa9117f3e6f2}[]
      Queries value:
HKLM \ software \ `microsoft \ `windows \ `current version \ `winevt \ publishers \ `\{67d07935-283a-4791-8f8d-1947, \ and \ 
 fa9117f3e6f2}[messagefilename]
     Queries value:
fa9117f3e6f2}[categorymessagefile]
     Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
 fa9117f3e6f2}[resourcefilename]
     Oueries value:
 HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67d07935-283a-4791-8f8d-
 fa9117f3e6f2}[parameterfilename]
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{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-1
 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\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-currentversion\channels\microsoft-windows-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[type]
      Queries value:
\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$}$-windows-$} \noindent \
```

wcmsvc/operational[enabled]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:loss-twindows-window-w---------------------------$

Queries value:

 $\label{thm:hklm} HKL^{M} software \mbox{\current} version \mbox{\current} channels \mbox{\current} version \mbox{\current} channels \mbox{\current} version \mbox{\current}$

Queries value:

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

Oueries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{$\mbox{$\mbox{$w$cmsvc/operational[clocktype]}$}} \\$

Queries value:

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

Oueries value

 $\label{thm:local-microsoft-windows-current-version-winevt-channels-microsoft-windows-wcmsvc/operational[level]$

Queries value:

 $\label{thm:loss-twindows-window-w---$

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \end{tabular} windows \soft-windows \end{tabular} wcmsvc/operational[maxsize]$

Oueries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc} windows \sc} windows \s$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc} windows \sc} with the constant \mbox{\sc} with \mbox{\sc} with the constant \mbox{\sc} with the constant \mbox{\sc} with the constant \mbox{\sc} with \mbox{\s$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \scalebox{\cdot wcmsvc/operational[isolation]} \\$

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc} windows \sc} windows \s$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\currentversion\winevt\channels\mbox{\currentversion\winevt\channels\mbox{\currentversion\winevt\channels\mbox{\currentversion\channels\mbox{\currentversion\channels\channels\mbox{\currentversion\channels\ch$

Queries value:

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

Queries value

 $\label{lem:hklm} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows-wcmsvc/diagnostic \cite{tilemax} \end{substitute}$

Queries value:

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

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{\sc} windows \screen \screen_hammon_ha$

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{\m

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value

 $\label{thm:local_hammels_microsoft_windows} HKLM \software \scalebox{$\operatorname{Microsoft-windows-local_hammels_microsoft-windows-local_hammels_hamm$

wcmsvc/diagnostic[level] Queries value: $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the substitution of the subs$ wcmsvc/diagnostic[keywordslower] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[keywordsupper] Oueries value: wcmsvc/diagnostic[controlguid] Queries value: $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ wcmsvc/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: $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity | Section | Section$ wcmsvc/diagnostic[retention] Oueries value: $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ wcmsvc/diagnostic[autobackuplogfiles] Queries value: $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ wcmsvc/diagnostic[file] $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ wcmsvc/diagnostic[filterid] Oueries value: $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ wcmsvc/diagnostic[isolation] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowswcmsvc/diagnostic[owningpublisher] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ wcmsvc/diagnostic[channelaccess] Queries value: $HKCR\ interface \ \{dbea162d-04e8-460f-8a0b-4a431715d9a3\}\ proxystubclsid32[]$ HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[] Queries value: Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{89fe8f40-cdce-464e-8217-664e-8217-664e-8217-664e-8217-6666-8666-86666-8666-86666-8666-86666-8666-86666-86666-8666-86666-86666-86666-86666-86666-86666-866$ 15ef97d4c7c3}[] Queries value: 15ef97d4c7c3}[messagefilename] Oueries value: $HKLM \setminus software \\ \mbox{89 fe8f40-cdce-$464e-$217-} \\$ 15ef97d4c7c3}[categorymessagefile] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{89fe8f40-cdce-464e-8217-1946, \ normalized \ publishers \ \ \}$ 15ef97d4c7c3}[resourcefilename] HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89fe8f40-cdce-464e-8217-15ef97d4c7c3}[parameterfilename] Queries value: 15ef97d4c7c3}[helplink] Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \ \{89fe8f40-cdce-464e-8217-4666e-8217-4666e-8217-4666e-8217-46666e-8217-66$ 15ef97d4c7c3}[enabled] Oueries value: 15ef97d4c7c3}[categorycount] $\label{thm:local_thm} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft-windows-crypto-windows-cry$ dpapi/operational[type] Queries value: $HKLM \ software \ microsoft-windows \ - crypto-like \ microsoft-windows \ - crypto-like \$ dpapi/operational[enabled] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[filemax] Queries value: $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows \ - crypto-part \ - crypto-par$ dpapi/operational[filecounter] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-part \ windows \ - crypto-part \ windows \ - crypto-part \ - cr$ dpapi/operational[buffersize] Queries value: $HKLM \ software \ `microsoft\ `windows\ `current version\ `winevt\ `channels\ `microsoft\ -windows\ -crypto-distribution\ `winevt\ `channels\ `winevt\ `winevt\ `winevt\ `channels\ `winevt\ `channels\ `winevt\ `channels\ `winevt\ `channels\ `winevt\ `winevt$ dpapi/operational[minbuffers] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/operational[maxbuffers] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-property \ channels \ - crypto-property \ - crypto-prop$ dpapi/operational[latency] Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-part \ windows \ - crypto-part \ windows \ - crypto-part \ - cr$

dpapi/operational[clocktype]

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:loss-twindows-crypto-def} HKLM \software \mbox{\currentversion-winevt-channels-microsoft-windows-crypto-dpapi/operational[maxsizeupper]}$

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-crypto-dpapi/operational [file]$

Queries value:

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

Queries value:

 $\label{thm:local_microsoft} HKLM \software \microsoft-windows-cryptodapi/operational[isolation]$

Queries value:

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

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows-cryptodapi/operational[channelaccess]$

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/backupkeysvc[enabled]

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-cryptodpapi/backupkeysvc[buffersize]$

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-crypto-dpapi/backupkeysvc[minbuffers]$

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[clocktype]

Oueries value

 $\label{thm:hammels} HKLM\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[sidtype]$

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-crypto-dpapi/backupkeysvc[level]

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-cryptodpapi/backupkeysvc[maxsizeupper]

Queries value:

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

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows-cryptodapai/backupkeys vc [autobackuplog files]$

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - crypto-property \ windows - crypto-property \ windows - crypto-property \ windows \ winevt \ windows \ windows \ windows \ windows \ winevt \ windows \ wi$ dpapi/debug[type]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-part \ windows \ - crypto-part \ windows \ - crypto-part \ - cr$ dpapi/debug[enabled]

Oueries value:

 $HKLM \ software \ microsoft-windows \ - crypto-like \ microsoft-windows \ - crypto-like \$ dpapi/debug[filemax]

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-part \ windows \ - crypto-part \ windows \ - crypto-part \ - cr$ dpapi/debug[minbuffers]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - crypto-part \ windows \ - crypto-part \ windows \ - crypto-part \ - cr$ dpapi/debug[maxbuffers]

Oueries value:

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

Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-crypto-property and the property of th$ dpapi/debug[clocktype]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -crypto-property \ -windows \ -wi$ dpapi/debug[maxsize]

Queries value:

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

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - crypto-property \ windows - crypto-property \ windows - crypto-property \ windows \ winevt \ windows \ windows \ windows \ windows \ winevt \ windows \ wi$ dpapi/debug[retention]

Oueries value:

 $\label{thm:local_hammels} \textbf{HKLM} \\ \textbf{Software} \\ \textbf{microsoft-windows-crypto-wi$ dpapi/debug[autobackuplogfiles]

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -crypto-part \ -windows \ -crypto-part \ -windows \ -crypto-part \ -windows \ -windo$ dpapi/debug[isolation]

Queries value:

 $HKLM \ software \ microsoft-windows \ - crypto-like \ microsoft-windows \ - crypto-like \$ dpapi/debug[owningpublisher]

Queries value:

dpapi/debug[channelaccess]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-1981, 1$ d5be7d52d6de}[]

Queries value:

 $HKLM \setminus software \\ \mbox{$microsoft\windows} \mbox{$currentversion\winevt\publishers} \\ \mbox{$q580d7dd-0379-4658-9870-1000} \\ \mbox{q} \mbo$ d5be7d52d6de}[messagefilename]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `winevt \ 'publishers \ '\{9580d7dd-0379-4658-9870-1981, \ winevt \ 'publishers' \ 'quad \ 'quad$ d5be7d52d6de}[categorymessagefile]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870d5be7d52d6de}[resourcefilename]

Queries value:

d5be7d52d6de}[parameterfilename]

Oueries value:

d5be7d52d6de}[helplink]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-1981, 1$ d5be7d52d6de}[enabled]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{9580d7dd-0379-4658-9870-1981, 1$ d5be7d52d6de}[categorvcount]

Oueries value:

autoconfig/operational[type]

Oueries value:

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

Queries value:

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

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/operational[filecounter]

Queries value:

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

Queries value:

autoconfig/operational[minbuffers]

Queries 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/operational[maxbuffers]

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

autoconfig/operational[maxsizeupper] Queries value:

 $HKLM \ software \ microsoft\ windows \ -windows - winevt\ -winevt\ -windows - winevt\ -winevt\ -winevt$ autoconfig/operational[retention] Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -wlandard \$ autoconfig/operational[autobackuplogfiles] Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-wlanautoconfig/operational[file] Oueries value:

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

Queries value:

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

Queries value:

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

Queries 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/operational[channelaccess]

Queries value:

autoconfig/diagnostic[type]

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

autoconfig/diagnostic[maxbuffers]

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[clocktype]$

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} With the lattice of the lat$

Oueries value

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[controlguid]$

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[maxsize]$

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[file]$

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[filterid]$

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[isolation]$

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[owningpublisher]$

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} wincrosoft-windows-wlan-autoconfig/diagnostic[channelaccess]$

Queries value: HKU\s-1-5-21-1923240461-1905901954-2556564120-

 $1001 \verb|\software\microsoft\windows| nt\currentversion\app compatflags \verb|\compatibility| is a superior of the compatibility of the com$

 $assistant \verb|\store|[c:\windows\temp\toggleservice32.exe]|$

Queries value:

HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

context logger[start]
 Queries value: HKLMY

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[flushthreshold]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[buffersize]

 $\label{logger} Queries \ value: \\ HKLM\system\current controlset\control\symi\autologger\circular\ kernel \\ context\ logger[minimumbuffers]$

 $Queries\ value: HKLM\system\currentcontrolset\control\symi\autologger\circular\ kernel\ context\ logger\[maximumbuffers\]$

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

context logger[filename]

 $\label{logger} Queries \ value: \\ HKLM\system\current controlset\control\symbol{\control} wmi\autologger\circular\ kernel context\ logger[enablekernelflags]$

 $\label{logger} Queries \ value: \ HKLM\system\current controlset\control\symmi\autologger\circular\ kernel context logger[stackwalkingfilter]$

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[clocktype]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[maxfilesize]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[logfilemode]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

context logger[disablerealtimepersistence]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

Queries value: HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-

af71-3e63d056f1741

Dueries value

 $\label{thm:local-section} HKCU software \end{area} HKCU software \end{area} in the sign of the section $$18-9926f41749ea \cunt[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{6bba3851-2c7e-4dea-8f54-31e5afd029e3\}[]$

Queries value:

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

Queries value:

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

Oueries value.

 $\label{thm:hammon} HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3\}[resourcefilename]}$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{6bba3851-2c7e-4dea-8f54-31e5afd029e3\} \ [parameter filename]$

Oueries value:

Queries value:

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

Oueries value

 $\label{thm:local-bound} HKLM \software \mbox{$6bba3851-2c7e-4dea-8f54-31e5afd029e3} [category count]$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{thm:hklm:microsoft} HKLM\software \ensuremath{\mathsf{Microsoft-windows-diagnosis-dps/debug[filecounter]}} debug[filecounter]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[retention]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosis-dps/debug[autobackuplogfiles]

Queries value:

 $\label{thm:local-prop} HKL^M\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnosis-dps/debug[file]$

Queries value:

 $\label{thm:local_hammels_microsoft-windows-diagnosis-dps/debug[filterid]} HKLM\software\mbox{\currentversion}\mbox{\winevt\channels\mbox{\windows-diagnosis-dps/debug[filterid]}}$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnosis - diagnosi - diagnosis - diagnosis - diagnosis - diagnosis - diagnosis - d$

dps/debug[isolation]

Queries value:

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} Current \label{lem:hklm} winevt \label{lem:hklm} Channels \label{lem:hklm} winevt \label{lem:hklm} Windows \label{lem:hklm} Constant \label{lem:hklm} Windows \label{lem:hkklm} Windows \label{lem:hkkl$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} Consideration also \label{lem:hklm} Is in the hard similar \label{lem:hklm} Windows \label{lem:hklm} Limit \label{lem:hklm} Windows \label{lem:hkklm} Windows \label{lem:hkklm$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:hammelsmicrosoft-windows-diagnosis-dps/operational[filterid]} HKLM\software\mbox{\currentversion}\winevt\channels\mbox{\currentversion}\winevt\channel\winevt\channel\winev$

Queries value:

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

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-diagnosis-dps/operational [owning publisher]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hkkm} HKLM \software \microsoft-windows-diagnosis-dps/analytic[filemax]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -diagnosis-diagnosi-$

dps/analytic[maxbuffers]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

Queries value:

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

Queries value:

 $\label{thm:local-microsoft-windows-diagnosis-dps/analytic[maxsizeupper]} HKLM\software\mbox{\currentversion}\winevt\channels\winevt\channel\winevt\c$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-publishers-form} HKLM \software \mbox{\cfc} 18ec0-96b1-4eba-961b-622caee05b0a \mbox{\cmale} [messagefilename]$

Queries value:

 $\label{thm:local-publishers} HKLM \software \mbox{\cfc} 18ec0-96b1-4eba-961b-622caee05b0a\\ [categorymessagefile]$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-prop} HKLM \software \mbox{$\cfc18ec0-96b1-4eba-961b-622caee05b0a}[helplink]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\ccrrentversion\winevt<page-header> publishers} \cfc18ec0-96b1-4eba-961b-622caee05b0a\class{\ccreentware} \class{\ccreentware} \class{\ccree$

Queries value:

 $\label{thm:local} HKLM \software \microsoft-windows \current version \winevt \channels \microsoft-windows - diagnostic specific mance/operational [type]$

Queries value:

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

Queries value:

 $\label{thm:local_microsoft} HKLM \software \microsoft-windows - diagnostic speciform ance/operational \cite{thm:local_filemax}.$

Queries value:

 $\label{thm:local_microsoft} HKLM \software \subseted in the local microsoft subseted in the$

Queries value:

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

Queries value

performance/operational[minbuffers]

Queries value:

 $\label{thm:local_maxbuffers} HKLM \software \subseted in the local maxbuffers \subseted in the local maxbuffer \subseted in the local maxbuf$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} Control \label{lem:hklm} Winevt \label{lem:hklm} Control \label{lem:hklm} Winevt \l$

Queries value:

 $HKLM \label{lem:hklm} In the latest and the lates$

Queries value:

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

Oueries value

 $\label{thm:local_hammels} HKLM \noinder{\noinder} windows - diagnostics-performance/operational[retention]$

Queries value:

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

Queries value:

 $\label{thm:hklm} \begin{tabular}{ll} HKLM \label{thklm:hklm:hklk} Which is the substitution of the subst$

Oueries value:

 $HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} In the label{lem:hklm} Winevt \label{lem:hklm} In the label{lem:hklm} Winevt \label{lem:hklm} In the label{lem:hklm} Hklm \label{lem:hklm} In the label{lem:hklm} In the label{lem:hkl$

Oueries value

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \sincos of t-windows - diagnostic s-performance/operational[owningpublisher]$

Queries value:

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

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic[type]} HKLM \software \mbox{\sc microsoft-windows-diagnostic-performance/diagnostic[type]}$

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft-windows - diagnostic superformance / diagnostic [file max]$

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic[filecounter]} HKLM \software \mbox{\sc windows-diagnostic-window-diagnosti$

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic[buffersize]} HKLM \software \mbox{\sc windows-diagnostic-window-diagnostic$

Queries value:

 $\label{thm:local-performance} HKLM \software \microsoft-windows-diagnostics-performance/diagnostic \microsoft-windows-diagnostic \microsoft-windows-$

Queries value:

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

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic[latency]} HKLM \software \end{time} with the constant of the constant$

Queries value:

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

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic[sidtype]} HKLM \software \microsoft-windows-diagnostic[sidtype]$

Oueries value:

 $\label{thm:local-microsoft-windows-diagnostic-performance/diagnostic[level]} HKLM \software \microsoft-windows-diagnostic-performance/diagnostic[level]$

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic[keywordslower]} HKLM \software \mbox{\sc microsoft-windows-diagnostic-wind$

Queries value:

 $\label{thm:local-performance} HKLM \software \microsoft-windows-diagnostics-performance/diagnostic \slashed \microsoft-windows-diagnostics-performance/diagnostic \slashed \$

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-diagnostic serformance/diagnostic \ [controlguid]$

Queries value

performance/diagnostic[maxsize]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \size windows \size under \size upon the lambda size upon \size upon$

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local-performance} HKLM \software \microsoft-windows-diagnostics-performance/diagnostic[file]$

Queries value:

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

Queries value:

Oueries value:

 $\label{thm:local-prop} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} M\software\\ \begin{tabular}{ll} HKL\begin{tabular}{ll} M\software\\ \begin{tabular}{ll} HKL\begin{tabular}{ll} HK$

Queries value:

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

Oueries value

 $\label{thm:hammelsmicrosoft-windows-diagnostics-performance/diagnostic/loopback[type]} HKLM\software\mbox{\c.} windows-diagnostic-windows-diagno$

Oueries value:

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

Queries value:

 $\label{lem:hklm} Hkl. M\ software \ microsoft-windows-diagnostics-performance/diagnostic/loopback \ [filemax]$

Oueries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostics-performance \/diagnostic \/loop \back[filecounter]$

Oueries value

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

Queries value:

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

Oueries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic/loopback[maxbuffers]} HKLM \software \mbox{\sc microsoft-windows-diagnostic-performance/diagnostic/loopback[maxbuffers]}$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostics-performance \/diagnostic \/losp \begin{tabular}{l} latency \end{tabular}$

Queries value:

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

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-diagnostics-performance/diagnostic/loopback[sidtype]$

Queries value:

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

Queries value:

 $\label{thm:local-performance} HKLM \software \microsoft-windows-diagnostics-performance/diagnostic/loopback [keywordslower]$

Queries value:

 $\label{thm:local-microsoft-windows-diagnostics-performance/diagnostic/loopback[keywordsupper]} HLMN software \end{array} in the thick of the thick$

Queries value

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} With \label{lem:hkklm} With \label{lem:hkklm$

Queries value:

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} With a microsoft-windows-diagnostic-performance/diagnostic/loopback[maxsizeupper]$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostics-performance \/diagnostic \/loop \back[retention]$

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[autobackuplogfiles]

Queries value:

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

Queries value:

 $\label{thm:local-performance} HKLM \software \microsoft-windows-diagnostics-performance/diagnostic/loopback \cite{literid}$

Queries value:

 $HKLM \ software \ microsoft-windows \ current version \ winevt \ channels \ microsoft-windows-diagnostic serformance/diagnostic/loopback [isolation]$

Queries value:

```
performance/diagnostic/loopback[owningpublisher]
  Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -diagnostics \ -diagnos
performance/diagnostic/loopback[channelaccess]
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]
  Queries value:
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus topip \setminus parameters [disable ip source routing]
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[arpretrycount]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[igmplevel]
  Oueries value:
  Oueries value:
                                    HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[igmpversion]|
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableaddrmaskreply]
HKLM\system\currentcontrolset\services\tcpip\parameters[disabletaskoffload]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablebcastarpreply]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledhcpmediasense]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable mediasen seevent log]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [enable multicast forwarding]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtudiscovery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpuserfc1122urgentpointer]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdataretransmissions]
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
  Queries value:
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \texttt{[tcptimedwaitdelay]}
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [tcpfinwait2delay]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtubhdetect]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[tcp1323opts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[qualifyingdestinationthreshold]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationsubnet]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [ipautoconfiguration mask]
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[arpuseethersnap]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[overridedefaultaddressselection]
  Queries value:
                                    HKLM\system\currentcontrolset\services\tcpip\parameters[maxuserport]
  Oueries value:
Oueries value:
55779daa70e9}[ipaddress]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[subnetmask]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[ipautoconfigurationaddress]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[ipautoconfigurationenabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[performrouterdiscovery]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[defaultgateway]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[defaultgatewaymetric]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[solicitationaddressbcast]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[usezerobroadcast]
  Oueries value:
55779daa70e9}[typeofinterface]
```

```
55779daa70e9}[mtu]
    Queries value:
55779daa70e9}[interfacemetric]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[tcpackfrequency]
    Oueries value:
55779daa70e9}[tcpdelackticks]
    Oueries value:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\dnscache[imagepath]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\dnscache[type]
                                                              HKLM\system\currentcontrolset\services\dnscache[start]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
    Oueries value:
    Queries value:
                                                              HKLM\system\currentcontrolset\services\dnscache[tag]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\dnscache[dependonservice]
                                                              HKLM\system\currentcontrolset\services\dnscache[dependongroup]
    Queries value:
    Oueries value:
                                                              HKLM\svstem\currentcontrolset\services\dnscache[group]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\dnscache[objectname]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[imagepath]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[type]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[start]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[errorcontrol]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[tag]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[dependonservice]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[dependongroup]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[group]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\p2pimsvc[objectname]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
                                                              HKLM\system\currentcontrolset\services\rpcss[objectname]
    Oueries value:
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\sppsvc[objectname]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\sppsvc[imagepath]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\sppsvc[wow64]
    Oueries value:
                                                              HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
    Queries value:
                                                              HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
                                                              HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
    Queries value:
    Oueries value:
                                                              HKLM\software\microsoft\windows\currentversion[programfilesdir]
    Queries value:
                                                              HKLM\software\microsoft\windows\currentversion[commonfilesdir]
    Queries value:
                                                              HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
    Queries value:
                                                              HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
    Oueries value:
                                                              HKLM\software\microsoft\windows\currentversion[programw6432dir]
                                                              HKLM\software\microsoft\windows\currentversion[commonw6432dir]
    Oueries value:
                                                              \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \end{tab
    Oueries value:
20[profileimagepath]
    Oueries value:
                                                              HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
    Oueries value:
                                                              shell folders[local appdata]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\sppsvc[environment]
    Queries value:
                                                              HKLM\system\currentcontrolset\services\sppsvc[startprotected]
                                                              HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\compatibility32[sppsvc]
   Queries value:
                                                              HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472c-
a5f9-f2bdfea0f156]
                                                              {\tt HKLM} \ system \verb|\currentcontrolset\| services \verb|\eventlog\| application \verb|\software| \\
   Oueries value:
protection platform service[providerguid]
    Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{e23b33b0-c8c9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9
f2bdfea0f156}[]
    Oueries value:
f2bdfea0f156}[messagefilename]
   Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-
f2bdfea0f156}[categorymessagefile]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-
f2bdfea0f156}[resourcefilename]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{e23b33b0-c8c9-472c-a5f9-microsoft\} \ windows \ version \ versio
f2bdfea0f156}[parameterfilename]
    Queries value:
f2bdfea0f156}[helplink]
f2bdfea0f156}[enabled]
    Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{e23b33b0-c8c9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9-472c-a5f9
f2bdfea0f156}[categorycount]
                                                             HKLM\software\microsoft\windows
   Oueries value:
\verb|nt\currentversion\software| protection platform[inactivity shutdown delay]| \\
    Oueries 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[]
    Queries value:
```

```
Oueries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10[]
  Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11[]
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12[]
  Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13[]
  Queries value:
 Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14[]
 Queries value:
                         HKLM\system\currentcontrolset\services\wsearch[objectname]
                         HKLM\system\currentcontrolset\services\http[objectname]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\winmgmt[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wscsvc[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wscsvc[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wscsvc[wow64]
 Queries value:
                         HKLM\system\currentcontrolset\services\wscsvc[requiredprivileges]
 Queries value:
                         HKLM\system\currentcontrolset\services\wscsvc\parameters[servicedll]
  Queries value:
HKLM\system\currentcontrolset\services\wscsvc\parameters[servicemanifest]
  Queries value:
                         HKLM\system\currentcontrolset\services\wscsvc\parameters[servicemain]
  Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15[]
 Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16[]
 Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17[]
 Oueries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18[]
                         HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-
 Queries value:
809b-2a87b70881f81
  Queries value:
                         8539-9230a44081a51
  Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19[]
 Queries value:
                         HKLM\software\microsoft\security center\svc[vistasp1]
  Queries value:
                         HKLM\software\microsoft\security center\svc[antivirusoverride]
                         HKLM\software\microsoft\security center\svc[antispywareoverride]
  Oueries value:
                         HKLM\software\microsoft\security center\svc[firewalloverride]
 Queries value:
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
 Oueries value:
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
 Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
  Oueries value:
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
 Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:
                         HKLM \ system \ wpa \ 8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2[]
 Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:
                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
                         HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
 Queries value:
 Queries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
 Queries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[serviceparameters]
 Oueries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[runas]
 Oueries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[activateatstorage]
 Oueries value:
 Oueries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[rotflags]
                         HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [appidflags]
 Oueries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[launchpermission]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\ole[legacyauthenticationlevel]
 Queries value:
                         {\tt HKLM \backslash software \backslash microsoft \backslash ole[legacyimpersonationlevel]}
 Queries value:
                         HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [authenticationlevel]
 Queries value:
                         HKCR \land appid \land \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} [remoteservername]
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[srptrustlevel]
  Oueries value:
 Queries value:
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}[preferredserverbitness]
                         HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[loadusersettings]
 Oueries value:
                         HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
 Oueries value:
                         HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
 Oueries value:
                         Queries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
 Queries value:
 Queries value:
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20[]
  Oueries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
  Queries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-
 Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries 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[]
 Oueries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
 Oueries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-
 Oueries value:
ce99a996d9ea}\inprocserver32[inprocserver32]
  Queries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\timescreer32[]
  Queries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
                         HKLM\software\microsoft\wbem\cimom[processid]
  Oueries value:
  Queries value:
                         HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
 Queries value:
                         HKLM\software\microsoft\wbem\cimom[contextlimit]
 Queries value:
                         HKLM\software\microsoft\wbem\cimom[objectlimit]
 Queries value:
                         HKLM\software\microsoft\wbem\cimom[identifierlimit]
                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21[]
 Oueries value:
                         HKCR\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
 Oueries value:
                         HKCR\clsid\{e7d35cfa-348b-485e-b524-
 Oueries value:
252725d697ca}\inprocserver32[inprocserver32]
                         Queries value:
 Oueries value:
                         HKCR\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[threadingmodel]
                         HKLM\software\microsoft\com3[gipactivitybypass]
  Queries value:
```

```
Queries value:
                                                                                                                                   HKCR\interface\{7c857801-7381-11cf-884d-00aa004b2e24}\proxystubclsid32[]
                                                                                                                                   HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}[]
          Queries value:
                                                                                                                                   HKCR\clsid\{71285c44-1dc0-11d2-b5fb-
          Queries value:
 00104b703efd}\inprocserver32[inprocserver32]
                                                                                                                                  HKCR\clsid\{71285c44-1dc0-11d2-b5fb-00104b703efd}\inprocserver32[]
         Queries value:
                                                                                                                                 HKCR\clsid\{71285c44-1dc0-11d2-b5fb-
         Oueries value:
00104b703efd}\inprocserver32[threadingmodel]
                                                                                                                                  HKCR\interface[interfacehelperdisableall]
         Oueries value:
         Queries value:
                                                                                                                                   HKCR\interface[interfacehelperdisableallforole32]
         Oueries value:
                                                                                                                                   HKCR\interface[interfacehelperdisabletypelib]
         Queries value:
                                                                                                                                   HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
          Queries value:
                                                                                                                                  00000000046}[interfacehelperdisableallforole32]
                                                                                                                                   HKCR\interface\{7c857801-7381-11cf-884d-
          Queries value:
 00aa004b2e24}[interfacehelperdisabletypelib]
        Queries value:
                                                                                                                                  HKCR\interface\{7c857801-7381-11cf-884d-
 00aa004b2e24}[interfacehelperdisableall]
                                                                                                                                 HKCR\interface\{7c857801-7381-11cf-884d-
        Queries value:
00aa004b2e24}[interfacehelperuser]
                                                                                                                                  HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
         Oueries value:
         Queries 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}\nprocserver32[]
          Oueries value:
                                                                                                                                   HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
 00104b703efd}\inprocserver32[threadingmodel]
         Queries value:
                                                                                                                                  HKCR \ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ proxystubclsid32[]
         Oueries value:
                                                                                                                                   HKCR\ interface \ \{423ec01e-2e35-11d2-b604-00104b703efd\}\ proxystubclsid32[]
         Queries value:
                                                                                                                                   HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}[]
                                                                                                                                 HKCR\clsid\{bfe18e9c-6d87-4450-b37c-
        Oueries value:
 e02f0b373803}\inprocserver32[inprocserver32]
                                                                                                                                  HKCR\clsid\{bfe18e9c-6d87-4450-b37c-e02f0b373803}\inprocserver32[]
         Oueries value:
                                                                                                                                 HKCR\clsid\{bfe18e9c-6d87-4450-b37c-
         Oueries value:
 e02f0b373803}\inprocserver32[threadingmodel]
        Queries value:
                                                                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22[]
         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}[category]
        Oueries value:
 9d55-7b8e7f157091}[name]
        Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parentfolder]
         Oueries value:
9d55-7b8e7f157091}[description]
        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}[relativepath]
 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}[parsingname]
        Oueries value:
9d55-7b8e7f157091}[infotip]
        Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localizedname]
         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}[icon]
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f1b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b32785-6fba-4fcf-10b3278-6fba-
 9d55-7b8e7f157091}[security]
        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}[streamresource]
        Queries value:
HKLM \label{lem:hklm} In the latest and the lates
9d55-7b8e7f157091}[streamresourcetype]
         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}[localredirectonly]
 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}[roamable1
        Queries value:
 9d55-7b8e7f157091}[precreate]
        Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fib32785-6fba-4fcf-
9d55-7b8e7f157091}[stream]
         Queries value:
9d55-7b8e7f157091}[publishexpandedpath]
        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}[attributes]
```

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

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

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

folders[local appdata]

Queries value:

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

Queries value:

9afe-ea3317b67173}[name]

Queries value:

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

Queries value:

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

Oueries value:

9afe-ea3317b67173}[relativepath]

Queries value:

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

9afe-ea3317b67173}[infotip]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1600\} \ and \$ 9afe-ea3317b67173}[localizedname]

Oueries value:

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

Queries value:

9afe-ea3317b67173}[security]

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

Queries value:

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

Oueries value:

9afe-ea3317b67173}[localredirectonly]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-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] Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1600\} \ and \ an arriver sion \ `explorer \ `folder descriptions \ `\{5e6c858f-0e22-4760-1600\} \ and \ an arriver sion \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `exp$ 9afe-ea3317b67173}[stream]

Oueries value:

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

9afe-ea3317b67173}[attributes]

Queries value:

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

Queries value:

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

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23[] Oueries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24[] Queries value: HKLM\svstem\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25[] Oueries value: Oueries value: $HKLM \verb|\software\microsoft\windows\currentversion\windows update \verb|\auto||$ update[auoptions]

Oueries value: $HKLM \ software \ `microsoft\ `windows \ `current version \ `windows update \ `auto'' \ and \ `windows \ `wi$ update[autoinstallminorupdates]

Queries value: $HKLM \ software \ `microsoft\ `windows \ `current version \ `windows update \ `auto'' \ and \ `windows \ `wi$ update[includerecommendedupdates]

Oueries value: $HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\w| indowsup date \verb|\auto| auto$ update[elevatenonadmins]

 ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus window supdate \setminus auto}$ Queries value:

update[configver]

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26[] Oueries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27[] Oueries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28[] Oueries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29[] Oueries value: Oueries value: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3[]

Queries value: HKLM\software\microsoft\security center[cval]

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

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]

Oueries value

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

HKLM\system\currentcontrolset\services\wscsvc\parameters[servicedllunloadonstop]

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

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

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

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

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

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

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

Queries value: HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-9[]

 $\label{thm:local-substance} HKLM \software \microsoft \windows \current version \winevt \publishers \end{4ee} 144e - 30ac - 3937643e - 37e - 3937643e - 37e - 37$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3\} \ [message filename]$

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3} \ [categorymessage file]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3\} \ [resource filename]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3\} \ [parameter filename]$

Queries value:

 $\label{thm:local-bound} HKLM \software \mbox{`windows`currentversion`winevt<page-header>publishers`{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[helplink]$

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \microsoft \windows \current version \winevt \publishers \end{4ee} 76bd8-3cf4-44a0-a0ac-3937643e37a3 \category \count]$

Queries value:

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

Queries value:

 $\label{thm:local_transform} HKLM \software \microsoft-windows-code integrity/operational[enabled]$

Queries value:

 $\label{thm:local} HKLM \noinder \noin$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:hklm:software:microsoft-windows-code} HKLM \software \mbox{\sc windows-code} integrity/operational [latency]$

Queries value:

 $\label{thm:hammels} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-code\cite{thm:hammels} and clocktype]$

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} Winevt \l$

Queries value:

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

Queries value:

 $\label{thm:loss-twindows} HKLM \software \mbox{\sc converted in the convertion} wine vt \channels \mbox{\sc convertion} exists a convertion \mbox{\sc conv$

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{$\mbox{w indows-code} integrity/operational[retention]}} \\$

Queries value:

 $\label{thm:local_microsoft} HKLM \software \microsoft-windows-code integrity/operational [autobackuplogfiles]$

Queries value:

 $\label{thm:loss-twindows-condition} HKLM \software \mbox{\sc windows-condeintegrity/operational[file]} \\$

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

Queries value:

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

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft-windows-currentversion| winevt\channels \end{tabular} icrosoft-windows-currentversion| winevt\channels \end{tabular} and the local content of the$ codeintegrity/operational[owningpublisher]

Oueries value:

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

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

codeintegrity/verbose[keywordslower] Queries value:

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

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

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

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

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[retention]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{windows$}$-windows-$} \noindent \$ codeintegrity/verbose[owningpublisher]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the second content of the second c$ codeintegrity/verbose[channelaccess]

Oueries value: HKLM\software\microsoft\windows

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

HKLM\software\microsoft\windows Queries value:

 $\verb|nt\currentversion| software protection platform \verb|plugins| modules \verb|179b8a65-b0f6-41d9-acea-down bloom bloom$ 12006ef9b32a[pluginfile]

HKLM\software\microsoft\windows Oueries value:

 $nt \verb|\current version| software protection platform \verb|\plugins| modules \verb|\c42d83ff-5958-4af4-a0dd-10| deleta a software protection platform \verb|\plugins| modules modu$ ba02fed39662[manifestfile]

```
Oueries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-
ba02fed39662[pluginfile]
            Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/active directory/1.0[module id]| and the province of the property of the proper
                                                                                                                                                                             HKLM\software\microsoft\windows
           Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
           Oueries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/bios/4.0[isservice]| | the software protection platform \verb| objects \verb| msft:rm/algorithm/bios/4.0[isservice]| | the software protection platform \verb| objects \verb| msft:rm/algorithm/bios/4.0[isservice]| | the software protection platform \verb| objects | objects \verb| objects | objects | objects | objects | objects | ob
           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 following the following platform of the followi
                                                                                                                                                                              HKLM\software\microsoft\windows
            Queries value:
\verb|nt\currentversion| software protection platform \verb|plugins\objects| msft:rm/algorithm/hwid/4.0[moduleid]| and the protection of the pro
                                                                                                                                                                              HKLM\software\microsoft\windows
 nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/phone/1.0[module id]| | the property of the prop
            Oueries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
                                                                                                                                                                             HKLM\software\microsoft\windows
            Queries value:
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/pkey/2009[module id]| | the software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/pkey/2009[module id]| | the software protection platform \verb| objects \verb| msft:rm/algorithm/pkey/2009[module id]| | the software protection platform \verb| objects \verb| msft:rm/algorithm/pkey/2009[module id]| | the software protection platform \verb| objects \verb| msft:rm/algorithm/pkey/2009[module id]| | the software protection platform \verb| objects \verb| ob
                                                                                                                                                                              HKLM\software\microsoft\windows
           Oueries value:
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/pkey/detect[moduleid]| and the province of the platform of the 
           Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
HKLM\software\microsoft\windows
            Queries value:
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/volume/1.0[module id]| | the following term of the following platform of th
                                                                                                                                                                              HKLM\software\microsoft\windows
nt \verb|\colored | logical terms | logical term
            Queries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[moduleid]
                                                                                                                                                                             HKLM\software\microsoft\windows
           Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[moduleid]
                                                                                                                                                                            HKLM\software\microsoft\windows
           Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[moduleid]
           Queries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[moduleid]
           Queries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt \verb|\colored| restriction restriction \verb|\colored| restriction r
             Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/collector/global/1.0[module id]| and the latest theorem \verb|\plugins| objects obje
            Oueries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[moduleid]
                                                                                                                                                                              HKLM\software\microsoft\windows
            Queries value:
nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft:spp/licenseacquisition| payload handler/eul/1.0[moduleid] | the protection of 
                                                                                                                                                                             HKLM\software\microsoft\windows
           Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[moduleid]
           Oueries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt \verb|\colored| likelihood | l
            Oueries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
 nt\corrent version\color{limits} it is not considered in the constant of the
                                                                                                                                                                              HKLM\software\microsoft\windows
            Queries value:
nt \verb|currentversion| software protection platform \verb|plugins| objects \verb|msft|: spp/license acquisition/payload handler/spc/1.0[module id]| and the plugins objects \verb|msft|: spp/license acquisition/payload handler/spc/1.0[module id]| and the plugins objects \verb|msft|: spp/license acquisition/payload handler/spc/1.0[module id]| and the plugins objects \verb|msft|: spp/license acquisition/payload handler/spc/1.0[module id]| and the plugins objects \verb|msft|: spp/license acquisition/payload handler/spc/1.0[module id]| and the plugins objects \verb|msft|: spp/license acquisition/payload handler/spc/1.0[module id]| and the plugins objects o
             Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/sequence/1.0[moduleid]| and the platform \verb|\plugins| objects obje
            Oueries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkev[moduleid]
                                                                                                                                                                             HKLM\software\microsoft\windows
           Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[moduleid]
           Oueries 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 \verb|\colored| later than $1$ and $1$ an
            Queries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
 nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[moduleid]
             Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
 nt\current version\colongled for m\plugins\objects\mbox{\sc spp/windows functionality/agent/7.0[isservice]}
            Queries value:
 HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
                                                                                                                                                                              HKLM\software\microsoft\windows
            Queries value:
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/active directory/1.0[isservice]|
                                                                                                                                                                              HKLM\software\microsoft\windows
           Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[isservice]
            Oueries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
HKLM\software\microsoft\windows
            Queries value:
Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/pkey/2005[isservice]| | the property of the pro
            Oueries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[isservice]
                                                                                                                                                                             HKLM\software\microsoft\windows
           Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[isservice]
                                                                                                                                                                            HKLM\software\microsoft\windows
           Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[isservice]
           Oueries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:rm/algorithm/volume/1.0[is service]| | the following the following plugins of the fol
            Oueries value:
                                                                                                                                                                             HKLM\software\microsoft\windows
 nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:spp/action/create process/1.0[isservice]|
                                                                                                                                                                              HKLM\software\microsoft\windows
            Queries value:
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/action/kernel/1.0[isservice]|
            Queries value:
                                                                                                                                                                              HKLM\software\microsoft\windows
```

```
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft:spp/action/reeval/1.0[is service]|
                                                                                  HKLM\software\microsoft\windows
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| msft: spp/action/vlactivate/1.0[isservice]| | the software protection platform \verb| objects \verb| objec
     Queries value:
                                                                                HKLM\software\microsoft\windows
nt \verb|\current version \verb|\software protection platform \verb|\plugins \verb|\software plugins \verb|\software plugins \verb|\software plugins | for the plugins \verb|\software plugins | for the plugins | for the
                                                                                HKLM\software\microsoft\windows
     Oueries value:
nt \verb|\colored| returned to the content of the con
     Oueries value:
                                                                                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]| | the software protection platform \verb| objects \verb| msft:spp/collector/kms/1.0[is service]| | the software protection platform \verb| objects \verb| msft:spp/collector/kms/1.0[is service]| | the software protection platform \verb| objects \verb| msft:spp/collector/kms/1.0[is service]| | the software protection platform \verb| objects \verb| msft:spp/collector/kms/1.0[is service]| | the software protection platform \verb| objects \verb| msft:spp/collector/kms/1.0[is service]| | the software protection platform \verb| objects \verb| o
                                                                                HKLM\software\microsoft\windows
      Queries value:
 \verb|mt\currentversion\software| protection platform \verb|plug| ins\objects\msft: spp/licenseacquisition/payload handler/eul/1.0[isservice]| | the protection of the protection of
                                                                                HKLM\software\microsoft\windows
 nt\corrent version\software protection platform\plugins\objects\mbox{\sc spp/licenseacquisition/payloadhandler/pa/1.0[isservice]}
      Oueries value:
                                                                                 HKLM\software\microsoft\windows
Queries value:
                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[isservice]
                                                                                HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[isservice]
     Queries value:
                                                                                HKLM\software\microsoft\windows
HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey[isservice]
                                                                                 HKLM\software\microsoft\windows
\verb|nt\currentversion| software protection platform \verb| plugins \verb| objects \verb| msft:spp/taskscheduler/1.0[isservice]| | the proof of the property of the propert
     Queries value:
                                                                                HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins objects \verb|\msft:spp/volume/services| kms/1.0[isservice]|
     Queries value:
                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[isservice]
                                                                                HKCU\software\microsoft\windows
     Queries value:
nt\currentversion\softwareprotectionplatform[kmshostconfig]
     Oueries value:
                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[enabletestvolumeintervals]
     Queries value:
                                                                                HKLM\software\microsoft\windows
\verb|nt\current version \verb| software protection platform[vlactivation interval]| \\
      Queries value:
                                                                                HKLM\software\microsoft\windows
\verb|nt\currentversion\software protection platform[vlrenewal interval]|
      Oueries value:
                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[actionlist]
     Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\sideby side[publisherpolicy change time]|
                                                                                HKLM\software\microsoft\windows
     Oueries value:
 nt\currentversion\softwareprotectionplatform[cachestore]
      Oueries value:
                                                                                  HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
      Queries value:
                                                                                  HKLM\system\setup\status[auditboot]
      Oueries value:
                                                                                  Queries value:
                                                                                  HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[compatibleids]
      Oueries value:
Queries value:
 HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00[compatibleids]
      Oueries value:
HKLM \setminus system \setminus current control set \setminus enum \setminus pci \setminus ven\_8086 \& dev\_7000 \& subsys\_00000000 \& rev\_00 \setminus 3 \& 267a616a \& 1 \& 08 [hardware id]
     Queries value:
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 7000&subsys 00000000&rev 00\3&267a616a&1&08[compatibleids]
                                                                                HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[hardwareid]
      Oueries value:
      Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[compatibleids]
       Oueries value:
                                                                                 HKLM \setminus system \setminus current control set \setminus enum \setminus acpi \setminus pnp0200 \setminus 4\&e03a844\&0 [hardwareid]
      Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[compatibleids]
                                                                                 HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[hardwareid]
       Queries value:
       Queries value:
 HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[compatibleids]
                                                                                HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[hardwareid]
     Queries value:
      Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[compatibleids]
     Queries value:
 HKLM\svstem\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1[hardwareid]
      Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[hardwareid]
       Oueries value:
      Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[compatibleids]
                                                                                 Queries value:
      Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[compatibleids]
     Queries 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]
     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 [compatible ids]
     Oueries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[hardwareid]
     Oueries value:
Queries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_
                                                                                                                                                                                                                                                                           __1.0.7.3_\5&34baf594&0&0.0.0[hardwareid]
      Queries value:
```

73e6154572dd}\inprocserver32[threadingmodel]

HKLM\system\currentcontrolset\control\productoptions[productpolicy] Oueries value:

HKLM\system\currentcontrolset\services\wpdbusenum\parameters[servicedllunloadonstop]

Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]

Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-

323e85a1ce84}\inprocserver32[inprocserver32]

Oueries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]

Queries value: HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-

323e85a1ce84}\inprocserver32[threadingmodel]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-

833b-323e85a1ce84]

Oueries value:

HKLM\software\policies\microsoft\internet Oueries value: explorer\security[disablesecuritysettingscheck]

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

explorer\security[disablefixsecuritysettings]

Queries value: HKCU\software\microsoft\internet

explorer\security[disablefixsecuritysettings]

Queries value: HKLM\software\microsoft\internet

explorer\security[disablefixsecuritysettings]

Queries value: HKLM\system\currentcontrolset\services\wscsvc[type] Oueries value: HKLM\system\currentcontrolset\services\wscsvc[start] Queries value: HKLM\system\currentcontrolset\services\wscsvc[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\wscsvc[tag]

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

Oueries value: HKLM\system\currentcontrolset\services\wscsvc[group]

 ${\tt HKLM \setminus software \setminus microsoft \setminus security \ center[autoup dated is ablenotify]}$ Queries value: Oueries value: ${\tt HKLM \setminus software \setminus microsoft \setminus security \ center[internet settings disable notify]}$

Queries value: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \action$ 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] Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.103[checksetting]

HKCU\software\microsoft\windows\currentversion\action Queries value: center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100[checksetting] HKCU\software\microsoft\windows\currentversion\action Queries value: center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.102[checksetting] $\label{thm:local_hammon} \verb+HKCU\+ software\+ microsoft\+ windows\+ current version\+ action$ Oueries value:

center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.104[checksetting] Oueries value: HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]

HKCR\clsid\{ca236752-2e77-4386-b63b-Queries value:

0e34774a413d}\inprocserver32[inprocserver32]

HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[] Queries value:

HKCR\clsid\{ca236752-2e77-4386-b63b-Oueries value:

0e34774a413d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\wbem\cimom[logging]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[a0ef609d-0a14-424c-

9270-3b2691a0a394]

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

86ba-948b704162201

Queries value: HKLM\software\microsoft\windows\windows error reporting[disabled] Oueries value: HKCU\software\microsoft\windows\windows error reporting[disabled]

Queries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]

Oueries value: HKCR\clsid\{88d96a05-f192-11d4-a65f-

0040963251e5}\inprocserver32[inprocserver32]

HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[] Queries value:

```
Queries value:
                                                                                                                                  HKCR\clsid\{88d96a05-f192-11d4-a65f-
 0040963251e5}\inprocserver32[threadingmodel]
                                                                                                                                    HKCU\software\microsoft\windows\currentversion\action
           Queries value:
  center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100[checksetting]
                                                                                                                                  HKCU\software\microsoft\windows\windows error
         Queries value:
 reporting[lastqueuepestertime]
                                                                                                                                  HKLM\software\microsoft\windows\windows error
          Oueries value:
 reporting[queuepesterinterval]
                                                                                                                                 HKCU\software\microsoft\windows\windows error
         Queries value:
  reporting[queuepesterinterval]
          Queries value:
                                                                                                                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ action
 center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting]
                                                                                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}[]
           Queries value:
          Queries value:
                                                                                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-
  499afcec98c4}\inprocserver32[inprocserver32]
                                                                                                                                  HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
           Oueries value:
          Queries value:
                                                                                                                                 HKCR\clsid\{c8e6f269-b90a-4053-a3be-
  499afcec98c4}\inprocserver32[threadingmodel]
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\action
         Queries value:
 center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4\}.check.0[checksetting]
                                                                                                                                  HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}[]
          Oueries value:
         Oueries value:
                                                                                                                                  HKCR\clsid\{088e8dfb-2464-4c21-bad2-
   f0aa6db5d4bc}\inprocserver32[inprocserver32]
           Queries value:
                                                                                                                                  HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[]
          Oueries value:
                                                                                                                                 HKCR\clsid\{088e8dfb-2464-4c21-bad2-
   f0aa6db5d4bc}\inprocserver32[threadingmodel]
                                                                                                                                 HKLM\software\policies\microsoft\windows\system[enablesmartscreen]
           Queries 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]
                                                                                                                                 HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}[]
         Queries value:
          Oueries value:
                                                                                                                                 HKCR\clsid\{d26de5c1-c061-43f7-9c40-
  7517526cf1c1}\inprocserver32[inprocserver32]
                                                                                                                                 HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[]
          Oueries value:
                                                                                                                                  HKCR\clsid\{d26de5c1-c061-43f7-9c40-
          Queries value:
 7517526cf1c1}\inprocserver32[threadingmodel]
          Queries value:
 \label{thm:local-continuous} HKCU \ software \ microsoft \ windows \ current version \ start up notify \ [enablest art up appnotification]
         Oueries value:
                                                                                                                                  HKCU\software\microsoft\windows\currentversion\action
  center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1\}.check.0[checksetting]
                                                                                                                                 HKCU\software\microsoft\windows\currentversion\action
          Queries value:
 center \verb|\providers| eventlog \verb|\end{|} \{01979c6a-42fa-414c-b8aa-eee2c8202018\} [lastknown state]
                                                                                                                                  HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
          Oueries value:
                                                                                                                                 HKCR\clsid\{900c0763-5cad-4a34-bc1f-
          Oueries value:
 40cd513679d5}\inprocserver32[inprocserver32]
                                                                                                                                 HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
          Queries value:
         Oueries value:
                                                                                                                                  HKCR\clsid\{900c0763-5cad-4a34-bc1f-
  40cd513679d5}\inprocserver32[threadingmodel]
          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 control of the contro
 windowsbackup/actioncenter[minbuffers]
          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
 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\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\channels\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[maxsize]
```

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

windowsbackup/actioncenter[maxsizeupper]

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-defined and the second content of the second c$ windowsbackup/actioncenter[retention]

Queries value:

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

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\micr$ windowsbackup/actioncenter[isolation]

Queries value:

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

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} windows \end{tabular} current version \end{tabular} winevt \end{tabular} cosoft-windows \end{tabular} and \end{tabular} winevt \end{tabular} winevt \end{tabular} cosoft-windows \end{tabular} and \end{tabular} winevt \end{tabular$ windowsbackup/actioncenter[channelaccess]

Oueries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100[checksetting] HKCU\software\microsoft\windows\currentversion\action Queries value: center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018\}.check.101[checksetting] 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\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsnetworkaccessprotection/whc[enabled]

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[filemax]

Queries value:

 $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{windows$}$-windows-$} \noindent \$ networkaccessprotection/whc[filecounter]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - winevt \cdot channels \setminus microsoft - windows - winevt \cdot channels \setminus microsoft - windows - winevt \cdot channels \cdot microsoft - winevt \cdot channels \cdot microsoft - windows - winevt \cdot channels \cdot microsoft - windows - winevt \cdot channels \cdot microsoft - winevt \cdot channels \cdot channels \cdot channels \cdot chan$ networkaccessprotection/whc[buffersize]

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{windows$}$-windows-$} \noindent \$ networkaccessprotection/whc[latency] Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the control of the contro$ networkaccessprotection/whc[maxsize]

Oueries value:

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\c$ networkaccessprotection/whc[maxsizeupper]

Oueries value:

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

Oueries value:

 $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{windows$}$-windows-$} \noindent \$ networkaccessprotection/whc[autobackuplogfiles]

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ networkaccessprotection/whc[file]

Queries value:

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

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - wind$ networkaccessprotection/whc[isolation]

Oueries value:

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

 $\label{thm:local_hammels_microsoft_windows} HKLM \software \mbox{$\mbox{$\mbox{windows$}$-windows-$} \noindent \$

networkaccessprotection/whc[channelaccess]

HKCU\software\microsoft\windows\currentversion\action

center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881\}.check.100[checksetting] Queries value:

HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate]

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \verb|\software\microsoft-windows\currentversion\winevt\channels\microsoft-windows-windows\columnwidth)| The software \verb|\software\microsoft-windows\channels\chann$ defender/whc[filemax]

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

Queries value:

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

Oueries value:

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

Queries value:

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

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

Queries value:

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

Oueries value:

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

Queries value:

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

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

Oueries value:

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

Oueries value:

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

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[retention]

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

HKCU\software\microsoft\windows\currentversion\action Oueries value: center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78\.check.101[checksetting]

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

center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate] Queries value:

scheduled/operational[type]

Queries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-continuous} \begin{tabular}{ll} HKLM \end{tabular} Software \verb|\microsoft-windows-diagnosis-diagno$ scheduled/operational[filecounter]

Queries value:

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

Oueries value:

scheduled/operational[minbuffers]

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

Oueries value

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

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - diagnosis-scheduled/operational[sidtype]$

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-microsoft-windows-diagnosis-scheduled/operational[maxsizeupper]} HKLM\software\mbox{\constraints} winevt\channels\mbox{\constraints} microsoft-windows-diagnosis-scheduled/operational[maxsizeupper]$

Queries value:

 $\label{thm:local_HKLM} HKLM \software \wincosoft \windows \current version \winevt \channels \wincosoft \windows \-diagnosis-scheduled \software \-diagnosis-scheduled \-diagnos$

Queries value:

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

Queries value:

 $\label{lem:hkkm} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - diagnosis-scheduled/operational[file]$

Oueries value:

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

Oueries value:

 $\label{thm:local_hammels} HKLM \software \microsoft-windows-diagnosis-scheduled/operational \cite{thm:local_hammels} is observed as the local_hammels \microsoft-windows-diagnosis-scheduled/operational \cite{thm:local_hammels} is observed as the local_hammels \microsoft-windows-diagnosis-scheduled/operational \cite{thm:local_hammels} is observed as the local_hammels \microsoft-windows-diagnosis-scheduled/operational \cite{thm:local_hammels} is observed \cite{thm:local_hammels} is observ$

Queries value:

 $\label{lem:hkkm} HKLM \software \wincosoft \windows \current version \winevt \channels \wincosoft \windows \-diagnosis-scheduled \/\ operational \[owning publisher]$

Queries value:

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

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

center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100[checksetting]

Queries value:

 $\label{thm:local-prop} HKLM \software \mbox{$\mbox{$\mbox{$\rm HKLM}$} irros of t-windows-task scheduler/maintenance [type]} \\$

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-windows} HKLM\software\mbox{\currentversion\winevt\channels\mbox{\currentversion}} winevt\channels\mbox{\currentversion\winevt\channels\mbox{\currentversion}} \\ tasks cheduler\mbox{\currentversion\$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

 $\label{thm:hklm} HKL^{M} software \mbox{\current} version \mbox{\current} channels \mbox{\current} version \mbox{\current} channels \mbox{\current} version \mbox{\current}$

Queries value:

 $\label{thm:loss-twindows} HKLM \software \mbox{\sc current} winevt \channels \mbox{\sc current} windows \ctasks \cheduler/maintenance [level]$

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \label{lem:hammels} HKLM \label{lem:hammels} If the lem is a single property of the lem$

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[retention]

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the control of the contro$ taskscheduler/maintenance[autobackuplogfiles]

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the control of the contro$ taskscheduler/maintenance[isolation]

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

Oueries value:

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

taskscheduler/maintenance[channelaccess] HKCU\software\microsoft\windows\currentversion\action Oueries value:

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

 $center\providers\eventlog \end{align*} \{134ea407-755d-4a93-b8a6-f290cd155023\} [lastknownstate]$ Queries value:

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

Queries value:

control panel/operational[enabled]

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

control panel/operational[clocktype] Queries value:

control panel/operational[sidtype]

Oueries value:

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

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

 $HKLM \ software \ microsoft\ windows \ current version \ winevt\ channels\ microsoft-windows-homegroup \ microsoft\ windows-homegroup \ microsoft\ window$

control panel/operational[maxsize]

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus winevt \setminus channels \setminus microsoft - windows - homegroup \cap version \setminus version \setminus$ control panel/operational[maxsizeupper]

Oueries value:

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

Queries value:

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

Queries value:

control panel/operational[file]

Queries value:

control panel/operational[filterid]

Queries value:

control panel/operational[isolation]

Oueries value:

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

Queries value:

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

HKCU\software\microsoft\windows\currentversion\action Oueries value: center\checks\{134ea407-755d-4a93-b8a6-f290cd155023\}.check.8001[checksetting] Queries value: HKCU\software\microsoft\windows\currentversion\action $center \verb|\providers| eventlog \verb|\c4efc9bb-2570-4821-8923-1bad317d2d4b| [lastknownstate]|$

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} Lem \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} his constant \label{lem:hklm} winevt \label{lem:hklm} Lem \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} Lem \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} his constant \label{lem:hklm} hklm \label{lklm} hklm$

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} crosoft-windows - security - spp-ux-notifications/actioncenter \cite{Action} action \cite{Action} action$

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-security-spp-uxnotifications/actioncenter[filemax]

Queries value:

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

Oueries value

Queries value:

Oueries value:

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

Oueries value:

Oueries value

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} - security - spp-ux-notifications/actioncenter \cite{Maxsize} \label{lem:hklm}$

Queries value:

Oueries value:

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winev \label{lem:hklm} Lem \label{lem:hklm} HKLM \label{lem:hklm} with \label{lem:hklm} with \label{lem:hklm} with \label{lem:hklm} hklm \label{lem:hklm} hklm \label{lem:hklm} with \label{lem:hklm} hklm \label{lklm} hklm \label{lk$

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value: HKCU\software\microsoft\wi

HKCU\software\microsoft\windows\currentversion\action

 $center \verb|\c4efc9bb-2570-4821-8923-1bad317d2d4b|.check.100[checksetting]|$

Queries value:

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Winevt \label{lem:hklm} \label{lem:h$

Queries value:

 $\label{lem:hklmsoftware} $$HKLM \circ ftware \ensurement version \en$

Queries value:

 $\label{thm:local-microsoft-windows-filehistory-core/whc[filecounter]} HKLM \software \mbox{\sc windows-filehistory-core/whc[filecounter]}$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-file \ history-core/\label{thm:local-prop} whe \cite{Controlguid}$

Queries value

 $\label{thm:hklm:microsoft-windows-filehistory-core/whc[maxsize]} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-filehistory-core/whc[maxsize]$

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} cosoft-windows-file history-core/whc[retention]$

Queries value:

Queries value:

 $\label{thm:loss} HKLM software \ensurements in \ensurements \ensurem$

Queries value:

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

Oueries value:

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

Oueries value:

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-file \ history-core/\label{thm:local-prop} whe \cite{Channel access} \end{microsoft-windows} \ description{ \cite{Channel access}} \ descripti$

Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100[checksetting]

Center\cnecks\{044/04d0-//80-11e0-ada3-18a90531a85a}.Cneck.100[cnecksetting]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[type]
Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[enabled]

Queries value:

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

Queries value:

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} Windows \label{lem:hklm} \label{lem:hklm} Windows \lab$

Queries value:

 $\label{thm:hklm} HKLM \label{thm:hklm} HKLM \label{thm:hklm} Which is the constant of the sum of$

Queries value

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

Queries value:

 $\label{thm:loss} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft - windows - ntfs/whc[latency]$

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Where \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} windows \label{lem:hklm} Where \label{lem:hklm} \label{lem:hklm} (Clock type)$

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[sidtype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[level]
Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} windows \label{lem:hklm} consoft-windows \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} hkll \label{lem:hklm} windows \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm}$

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-ntfs/whc[retention]

Queries value:

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

Oueries value:

 $\label{thm:local_hammon_hammon} HKL M \ software \ microsoft-windows-ntfs/whc[file] Oueries value:$

 $HKLM \verb|\software\microsoft-windows-currentversion\winevt\channels\microsoft-windows-currentversion\channels\microsoft-windows-current\end{windows-currentversion\channels\microsoft-windows-currentv$ ntfs/whc[filterid] $HKLM \verb|\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-linearity with the control of the contro$ ntfs/whc[isolation] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[owningpublisher] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsntfs/whc[channelaccess] Queries value: $\label{lem:hkcu} \verb+KCU\software\microsoft\windows\currentversion\action$ center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482\}.check.100[checksetting] Queries value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}[lastknownstate] $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -shell-like \ microsoft\ -windows\ -shell-like \ -windows\ -shell\ -shell \ -windows\ -shell\ -shell\$ connectedaccountstate/actioncenter[type] Queries value: $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus winevt \setminus channels \setminus microsoft - windows - shell-shear version - windows - window$ connectedaccountstate/actioncenter[enabled] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[filemax] Oueries value: $HKLM \ software \ microsoft\ windows\ - shell-like \ microsoft\ - windows\ - shell-like \ microsoft\ - windows\ - shell-like \ microsoft\ - windows\ - shell-like \ - windows\ - wi$ connectedaccountstate/actioncenter[filecounter] Queries value: $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -shell-like \ microsoft\ -windows\ -shell-like \ -windows\ -shell-like \ -windows\ -shell-like \ -windows\ -shell-like \ -windows\ -windows$ connectedaccountstate/actioncenter[buffersize] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[minbuffers] Oueries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[maxbuffers] Oueries value: $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -shell-like \ microsoft\ -windows\ -shell-like \ -win$ connectedaccountstate/actioncenter[latency] Oueries value: connectedaccountstate/actioncenter[clocktype] Queries value: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[sidtype] Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -shell-like \ -windows \ -win$ connectedaccountstate/actioncenter[level] Oueries value:

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

 $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -shell-like \ microsoft\ -windows\ -shell-like \ -windows\ -shell\ -shell \ -windows\ -shell\ -windows\ -shell\ -shell\ -windows\ -shell\ -shell\ -shell\ -windows\ -shell\ -shell\$ connectedaccountstate/actioncenter[controlguid]

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[maxsize]

Oueries value:

 $HKLM \label{lem:hkk} LM \label{lem:hkkk} Which is the software \label{lem:hkkkk} windows \label{lem:hkkkk} Software \label{lem:hkkkkkk} windows \label{lem:hkkkkkkkkkk}.$ connectedaccountstate/actioncenter[maxsizeupper]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[retention]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -shell-like \ -shell-like$ connectedaccountstate/actioncenter[autobackuplogfiles]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -shell-like \ -windows \ -win$ connectedaccountstate/actioncenter[file]

Oueries value:

connectedaccountstate/actioncenter[filterid]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-shellconnectedaccountstate/actioncenter[isolation]

Oueries value:

connectedaccountstate/actioncenter[owningpublisher]

 $HKLM \ software \ microsoft\ windows\ current version \ winevt\ channels\ microsoft\ -windows\ -shell-like \ microsoft\ -windows\ -shell-like \ -windows\ -shell\ -shell\ -shell\ -windows\ -shell\ -shell\ -windows\ -shell\ -shell$ 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\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[type]

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[enabled]

Queries value:

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

Queries value:

 $\label{thm:loss-twindows} HKLM \software \ensurements in winevt \channels \ensurements in the context of the$

Oueries value

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[minbuffers]

Oueries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[latency]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[clocktype]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[sidtype]

Oueries value:

 $\label{thm:local_hammon_hammon} HKLM \software \microsoft-windows-userpnp/actioncenter[level]$

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} wincrosoft-windows-userpnp/actioncenter[controlguid]$

Queries value

 $\label{thm:loss-twindows} HKLM \software \mbox{\sc urrentversion} winevt \channels \mbox{\sc urrentversion} winevt \channels \mbox{\sc urrentversion} winevt \channels \mbox{\sc urrentversion} \cline{The proposed of the p$

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[autobackuplogfiles]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windowsuserpnp/actioncenter[file]

Queries value:

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

Queries value:

 $\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{$\mbox{$\mbox{$w$} indows-userpnp/actioncenter}[isolation]} \\$

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-userpnp/action center \cite{lowning} publisher]$

Queries value:

 $\label{thm:loss-twindows} HKLM \software \mbox{\sc} windows \sc} userpnp/action center[channel access]$

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft-windows \scurrent version \microsoft-windows-storage spaces-management \scalebox{\classifications} whice \scalebox{\classifications} is the local \scalebox{\classification} whice \scalebox{\classifications} is the local \scalebox{\classification} whice \scalebox{\classifications} is the local \scalebox{\classification} whice \scalebox{\classification} is the local \scalebox{\classification} with \scalebox{\classification} with \scalebox{\classification} whice \scalebox{\classification} with \scalebox{\classification}$

Queries value:

 $\label{thm:local-prop} HKLM \software \mbox{$\mbox{$\mbox{$\rm M$icrosoft-windows-storagespaces-managementagent/whc[enabled]}} \\$

Oueries value

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

Queries value:

\defies value.
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc[filecounter]

Queries value:

Queries variue.

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-storagespacesmanagementagent/whc[buffersize]

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-storage spaces-management agent/whc[minbuffers]$

Queries value:

 $\label{thm:loss-twindows-storage-spaces} HKLM \software \mbox{$$

Queries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-storage spaces-management agent/whc[latency]$

Queries value:

 $\label{thm:local-prop} HKLM \software \mbox{$\mbox{}\mbox{$\mbox{\mbo

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\sc} windows \screen \screen \screen \screen} winevt \channels \mbox{\sc} microsoft-windows-storage spaces-management \screen \screen$

Oueries value:

 $\label{thm:loss} HKLM \software \microsoft-windows-storage spaces-management agent/whc[level]$

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ -windows \ -storage spaces - the software \ -windows \ -window$ managementagent/whc[controlguid]

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constraints \ described and \ described \ de$ managementagent/whc[maxsize]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - storage spaces - windows - windows$ managementagent/whc[maxsizeupper]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constant \ channels \ -storage \ -s$ managementagent/whc[retention]

Queries value:

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

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constraints \ described and \ described \ de$ managementagent/whc[file]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces \ -storage \ -storage \ spaces \ -storage \ -stora$ managementagent/whc[filterid]

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[isolation]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constraints \ described and \ described \ de$ managementagent/whc[owningpublisher]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -storage spaces - the sum \ constant \ channels \ -storage \ -s$ managementagent/whc[channelaccess]

HKCU\software\microsoft\windows\currentversion\action Oueries value: center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100[checksetting]

Sets/Creates value:

HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]

Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[ndismajorversion] Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[ndisminorversion] Sets/Creates value: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ native wifip[driver major version]|$ Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[driverminorversion] HKLM\system\currentcontrolset\services\ndisuio[ndismajorversion] Sets/Creates value: 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\system\currentcontrolset\services\tcpip\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\software\microsoft\windows Value changes:

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\control\wmi\autologger\circular kernel

context logger[status]

Value changes:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ user as sist \ \{cebff5cd-ace2-4f4f-9178-4f4f-$ 9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]

Value changes:

9926f41749ea}\count[hrzr_pgyfrffvba]

Value changes:

Value changes:

HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection] Value changes:

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

Value changes: 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: ${\tt HKLM \setminus software \setminus microsoft \setminus security \ center \setminus svc[antispyware override]}$ Value changes: HKLM\software\microsoft\security center\svc[firewalloverride]

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

Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[licstatusarray] HKLM\software\microsoft\windows Value changes: nt\currentversion\softwareprotectionplatform[actionlist]

Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting] HKCU\software\microsoft\windows\currentversion\action Value changes: center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.103[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.102[checksetting]