Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID: 831 Risk Level: 10

2016-05-18 10:43:53 (UTC Date Processed:

Processing Time: 63.41 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"

Sample ID: 3331 Type: basic Owner: admin

Label: 1be5bc13fd1cf615a95feec0c5b7fd13 Date Added 2016-05-18 10:30:52 (UTC)

PE32:win32:gui File Type: File Size:

201728 bytes 1be5bc13fd1cf615a95feec0c5b7fd13 MD5:

SHA256: 10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347

Description:

Pattern Matching Results

Modifies registry autorun entries

Writes to memory of system processes Writes to system32 folder

5 Abnormal sleep detected

Injects thread into Windows process 3 Connects to local host

6 Changes Winsock providers

10 Creates malicious events: ZeroAccess [Rootkit]

4 Terminates process under Windows subfolder

4 Reads process memory

3 Long sleep detected

5 Installs service

Process/Thread Events

Creates process: C:\Windows\bfe.dll,BfeOnServiceStartTypeChange] C:\Windows\system32\rundll32.exe [C:\Windows\system32\rundll32.exe

Creates process:

C:\Windows\SysWOW64\cmd.exe ["C:\Windows\system32\cmd.exe"] \SvstemRoot\Svstem32\Conhost.exe [\??\C:\Windows\svstem32\conhost.exe Creates process:

0xffffffff]

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

C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe]
PID:1780 C:\Windows\Sys\WO\W64\calc.exe Creates process:

Reads from process: PID:1120 C:\Windows\explorer.exe
PID:480 C:\Windows\System32\services.exe Writes to process: Writes to process: PID:2148 C:\Windows\SysWOW64\cmd.exe Writes to process:

C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exeC:\Windows\SysWOW64\cmd.exe Terminates process

Terminates process: C:\Windows\System32\conhost.exe
C:\Windows\System32\rundll32.exe Terminates process: Terminates process: Creates remote thread: Creates remote thread: C:\Windows\explorer.exe
C:\Windows\System32\services.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \BaseNamedObjects\DBWinMutex

\Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{OC5AB9CD-

2F90-6754-8374-21D4DAB28CC13 Creates event: \Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{A3D35150-

6823-4462-8C6E-7417FF841D783 \BaseNamedObjects\\BaseNamedObjects\\Restricted\\{A3D35150-6823-4462-8C6E-

Creates event: 7417FF841D77}

\Sessions\1\BaseNamedObjects\PRS_EXTERNAL_CHECK_CHANGED_NOTIFY Creates event

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

File System Events

Creates C:\\$Recycle.Bin\

C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001
C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-Creates

Creates

1001\\$915369118a4888a39e2f92dbd118adb3 Creates: C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-

1001\\$915369118a4888a39e2f92dbd118adb3\L Creates: C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-Creates 1001\\$915369118a4888a39e2f92dbd118adb3\U

C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-

1001\\$915369118a4888a39e2f92dbd118adb3\@ C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-Creates

1001\\$915369118a4888a39e2f92dbd118adb3\n

C:\\$Recycle.Bin\S-1-5-18 Creates:

C:\\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3 C:\\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3\L Creates \\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3\U Creates Creates C:\\$Recycle.Bin\S-1-5-18\\$915369118a488a39e2f92dbd118adb3\@ C:\\$Recycle.Bin\S-1-5-18\\$915369118a488a39e2f92dbd118adb3\n

Creates Creates C:GAC MSIL

C:\Windows\assembly\GAC Creates

Creates C:GAC 32 Creates:

C:\Windows\assembly\GAC_64\Desktop.ini
C:\Windows\assembly\GAC_32\Desktop.ini Creates Creates:

C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558 C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513 Creates: Creates:

\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles \Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC Creates Creates:

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

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

Opens: :\Windows\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-CFDFB467.pf

Opens: C:\Windows

Opens: \Windows\System32\wow64.dll Opens C:\Windows\SysWOW64

Opens

C:\Windows\SysWOW64\apphelp.dll

```
C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
  Opens
                                  \Windows\SysWOW64\ntdll.dll
  Opens:
                               C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KernelBase.dll
  Opens:
  Opens
                               C:\Windows\apppatch\sysmain.sdb
C:\Windows\SysWOW64\sechost.dll
  Opens:
  Opens
  Opens:
                                 :\Windows\SysWOW64\msvcrt.dll
:\Windows\SysWOW64\gdi32.dll
  Opens:
                               C:\Windows\SysWOW64\user32.dll
                                  \Windows\SysWOW64\shlwapi.dll
  Opens
                               C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Windows\SysWOW64\cryptbase.dll
  Opens:
  Opens
                               C:\Windows\SysWOW64\sspicli.dll
C:\Windows\SysWOW64\rpcrt4.dll
  Opens
  Opens
                                 \Windows\SysWOW64\advapi32.dll
                               C:\Windows\SysWOW64\imm32.dll
  Opens
  Opens:
                                  \Windows\SysWOW64\msctf.dll
  Opens
                               C:\Windows\SysWOW64\includeincludeincludeincludeincludeincludei
                                  \Windows\Globalization\Sorting\SortDefault.nls
  Opens:
  Opens:
                               C:\Windows\SysWOW64\cabinet.dll
                                  \Windows\SysWOW64\nsi.dll
  Opens
                               C:\Windows\SysWOW64\ws2_32.dll
  Opens:
                                  \Windows\SysWOW64\mswsock.dll
  Opens
  Opens
                               C:\Windows\SysWOW64\cryptsp.dll
                                  \Windows\SysWOW64\rsaenh.dll
  Opens:
Opens: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
  Opens
                               C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
                               C:\Windows\assembly
  Opens:
                               C:\Windows\assembly\GAC_32\Desktop.ini
C:\Windows\assembly\GAC_64\Desktop.ini
  Opens
  Opens
                               C:\Windows\System32\cryptsp.dll
C:\Windows\System32\rsaenh.dll
  Opens
  Opens:
                                 \$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\U
  Opens:
  Opens
  Opens:
                                  \Windows\System32\rundll32.exe
                               C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
  Opens:
                                  \Windows\System32
  Opens:
                               C:\Windows\Svstem32\en-US\rundl132.exe.mui
  Opens:
                                  \Windows\System32\BFE.DLL
  Opens:
                               C:\Windows\system32\bfe.dll.123.Manifest
C:\Windows\system32\bfe.dll.124.Manifest
  Opens:
  Opens:
                               C:\Windows\system32\bfe.dll.2.Manifest
C:\Windows\System32\authz.dll
  Opens:
  Opens
  Opens:
                               C:\Windows\System32\dnsapi.dll
C:\Windows\System32\sechost.dll
  Opens
  Opens
                               C:\Windows\SysWOW64\cmd.exe
  Opens:
                               C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
  Opens
  Opens
                               C:\Windows\Globalization
  Opens
  Opens:
                                 :\Windows\Globalization\Sorting
                                  \Windows\SysWOW64\wbe
  Opens:
                               C:\Windows\Svstem32\ntdll.dll
  Opens:
  Opens:
                                  \Windows\System32\wow64win.dll
  Opens:
                               C:\Windows\System32\wow64cpu.dll
                                  \Windows\System32\kernel32.dll
  Opens
  Opens
                               C:\Windows\System32\user32.dll
                                  \Windows\System32\locale.nls
  Opens
                               C:\Windows\SysWOW64\wbem\WMIC.exe
C:\Windows\System32\conhost.exe
  Opens:
  Opens
                               C:\Windows\System32\combase.dll
C:\Windows\System32\en-US\conhost.exe.mui
  Opens:
  Opens:
  Opens:
                               C:\Windows\System32\ole32.dll
C:\Windows\System32\uxtheme.dll
  Opens
                               C:\Windows\System32\cmd.exe
C:\Windows\System32\en-US\cmd.exe.mui
  Opens:
                               C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\@
                               C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
  Opens
  Opens:
                               C:\Windows\Svstem32\taskhost.exe
                                  \Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
  Opens:
  Opens:
                               C:\Windows\Prefetch\TASKHOST.EXE-CC5C42C1.pf
  Opens:
                                  \Windows\Performance
  Opens:
                               C:\Windows\Performance\WinSAT
                                  \Windows\System32\en-US
  Opens
                               C:\Windows\System32\KernelBase.dll
C:\Windows\System32\msvcrt.dll
  Opens:
  Opens
                               C:\Windows\System32\rpcrt4.dll
C:\Windows\System32\oleaut32.dll
  Opens:
  Opens
                               C:\Windows\System32\rpcss.dll
C:\Windows\System32\cryptbase.dll
  Opens:
  Opens:
                               C:\Windows\System32\bcryptprimitives.dll
C:\Windows\System32\gdi32.dll
C:\Windows\System32\en-US\taskhost.exe.mui
  Opens:
  Opens
  Opens
  Opens:
                               C:\Windows\Svstem32\clbcatq.dll
                                  \Windows\System32\shlwapi.dll
  Opens:
  Opens:
                               C:\Windows\Svstem32\shell32.dll
                                  \Windows\System32\advapi32.dll
  Opens:
  Opens:
                               C:\Windows\System32\SHCore.dll
  Opens
                                  \Windows\System32\MemoryDiagnostic.dll
                               C:\Windows\System32\fhsvcctl.dll
C:\Windows\System32\regidle.dll
  Opens:
  Opens
  Opens:
                               C:\Windows\System32\pstask.dl1
C:\Windows\System32\imm32.dl1
  Opens
                               C:\Windows\System32\dwmapi.dll
C:\Windows\System32\wdi.dll
  Opens:
  Opens:
                               C:\Windows\System32\radarrs.dll
C:\Windows\WinSxS\amd64_microsoft.windows.common-
  Opens:
  Opens
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comct132.dll
Opens: C:\Windows\System32\RstrtMgr.dll
                               C:\Windows\System32\wer.dll
  Opens:
                               C:\Windows\System32\version.dll
  Opens:
                                  \Windows\System32\ncrypt.dll
  Opens:
  Opens:
                               C:\Windows\System32\bcrypt.dll
                               C:\Windows\System32\ntasn1.dll
  Opens
  Opens
                               C:\Windows\WindowsShell.Manifest
  Opens
                               C:\Windows\System32\en-US\radarrs.dll.mui
```

```
Opens
\label{lem:condition} C: \dot{\textbf{U}} sers \land \textbf{Admin} \land \textbf{PDData} \land \textbf{Roaming} \land \textbf{Microsoft} \land \textbf{Windows} \land \textbf{Themes} \land \textbf{CachedFiles} \land \textbf{Cache
      Opens:
                                                                                          C:\Users\desktop.ini
                                                                                          C:\Users
       Opens
      Opens:
                                                                                          C:\Users\Admin
                                                                                          C:\Users\Admin\AppData
      Opens:
      Opens:
                                                                                          C:\Users\Admin\AppData\Roaming
C:\Users\Admin\AppData\Roaming\Microsoft\desktop.ini
      Opens:
                                                                                          C:\Users\Admin\AppData\Roaming\Microsoft
C:\Users\Admin\AppData\Roaming\Microsoft\Windows
      Opens:
                                                                                          C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries
      Opens:
      Opens:
      Opens:
                                                                                          C:\Users\Admin\Desktop\desktop.ini
                                                                                          C:\Users\Public\desktop.ini
      Opens:
                                                                                          C:\Users\Public
       Opens:
                                                                                          C:\Users\Public\Desktop\desktop.ini
      Opens:
       Opens:
                                                                                           C:\Windows\ServiceProfiles
      Opens:
                                                                                          C:\Windows\System32\sppsyc.exe
       Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~en
US~6.2.9200.16384.cat
     Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens
00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Hyper-V-Management-PowerShell-Package-net-} \\ 31bf3856ad364e35-amd64-en-defined by the control of the contr
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-minkernel-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Hyper-V-Package-termsrv-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat} \\ \mbox{Continuous of the continuous of the conti
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Virtualization-Client-Interop-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-Anytime-Upgrade-Package-31bf3856ad364e35-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64-en-2005-amd64
US~6.2.9200.16384.cat
Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-Anytime-Upgrade- | Microsoft-Windows-Windows- | Microsoft-Windows- | Microsoft-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-Anytime-Upgrade-Results-Package} {\tt ~31bf3856ad364e35} {\tt ~amd64} {\tt ~en-Comparison} {\tt ~amd64-en-Comparison} {\tt ~amd64-en-Comparis
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-Package-31bf3856ad364e35~amd64~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore
```

```
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
Opens: C: \verb|Windows\System32| catroot\ \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ |Microsoft-Windows-ApisetNamespace-Minio-1999 | Minio-1999 | Minio
Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE\} \verb+\Microsoft-Windows-ApisetNamespace-Minkernel-Package \verb+^31bf3856 ad 364 e 35 \verb+^amd 64 \verb+^en-Package \verb+^31bf3856 ad 364 e 35 \verb+^amd 64 \verb+^en-Package \verb+^amd 64 \verb+^en-Package \verb+^amd 64 + amd 64 +
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-
Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
\label{lem:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens
US~6.2.9200.16384.cat
       Opens
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-
Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-ApisetNamespace-WOW64-Ap
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-ApisetNamespace-WOW64-Base-Package} {\tt ~31bf3856ad364e35-amd64-en-Base-Package} {\tt ~31bf3866ad364-amd64-en-Base-Package} 
US~6.2.9200.16384.cat
Opens: C: \verb|Windows| System32| catroot| \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-ApisetNamespace-WOW64-Base-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-ApisetNamespace-WOW64-Base-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-ApisetNamespace-WOW64-Base-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-ApisetNamespace-WOW64-Base-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-ApisetNamespace-WOW64-Base-11D1-85E5-00C04FC295EE] \\ | Microsoft-Windows-Microsoft-WOW64-Base-11D1-85E5-00C04FC295EE] \\ | Microsoft-WOW64-00C04FC295EE] \\ | Microsoft-WOW64-0
Package~31bf3856ad364e35~amd64~~c.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-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-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \label{lem:condition} Microsoft-Windows-ApisetNamespace-WOW64-Com-Package-31bf3856ad364e35-amd64-ce.2.9200.16384.cat
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
Opens:
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-
Package~31bf3856ad364e35~amd64~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
 Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295E}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
       Opens:
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-10c064 \\ \sim 
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\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Backup-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Basic-Http-Minio-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
       Opens:
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel-31bf3856ad364e35-amd64~en-
```

```
US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel-31bf3856ad364e35-amd64--6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
       Opens:
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Branding-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Branding-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-Branding-Professional \\ WMC-Package \sim 31bf3856ad364e35 \sim amd \\ 64 \sim en-package 
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Branding-Professional\WMC-Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \texttt{Microsoft-Windows-BusinessScanning-Feature-Package-admin-31bf3856ad364e35-amd64-en-2000} \\ \texttt{Microsoft-Windows-Business-Microsoft-Windows-Business-Microsoft-Windows-Business-Microsoft-Windows-Business-Microsoft-Windows-Business-Microsoft-Windows-Business-Microsoft-Windows-Business-Microsoft-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Win
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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-Business Scanning-Feature-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^energy \\ ^amd64 \\ 
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package
 base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 US~6.2.9200.16384.cat
                                                                                                                   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-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
  US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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 \sim 31bf3856ad364e35 \sim amd 64 \sim n-1000 \\ Microsoft-Windows-Client-Drivers-Package-multimedia \sim 31bf3856ad364e35 \\ \sim amd 64 \sim n-1000 \\ Microsoft-Windows-Client-Drivers-Package-multimedia \sim 31bf3856ad364e35 \\ \sim amd 64 \sim n-1000 \\ Microsoft-Windows-Client-Drivers-Package-multimedia \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \sim n-1000 \\ Microsoft-Windows-Client-Drivers-Package-multimedia \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \sim n-1000 \\ Microsoft-Windows-Client-Drivers-Package-multimedia \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \sim n-1000 \\ Microsoft-Windows-Client-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-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
                                                                                                                   C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
 multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
 00C04FC295EE\} \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Client-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Drivers-Package-net \sim 31bf3856ad364e35 \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Drivers-Package-net \sim amd 64 \sim en-100c04FC295EE \land Microsoft-Windows-Drivers-Package-net \sim amd 64 \sim en-100c04FC295EE \sim amd 64 \sim en-100c04FC2
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package
 net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-printscan~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
 printscan-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
        Opens:
                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~en-detection for the control of the
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
  admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                   C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
  00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C: \windows\system32\catroot\space{2.5cm} Coc04FC295EE\space{2.5cm} Microsoft-Windows-Client-Features-Package-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364e35-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf3856ad364-amd64-en-base-31bf386ad364-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64-en-
  US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE\} \\ Microsoft-Windows-Client-Features-Package-drivers-31bf3856ad364e35-amd64-ended from the control of the contr
 US~6.2.9200.16384.cat
                                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

00C04FC295EE}\Microsoft-Windows-Client-Features-Package

```
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C: \verb|Windows| System32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-Client-Features-Package-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-
ds~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-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
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-100C04FC295EE}
 inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Client-Features-Package-mergedcomponents-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mincore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C: \verb|Windows| System32| catroot| \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-Client-Features-Package-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3856ad364e35-amd64-en-day-minio-31bf3866ad364e35-amd64-en-day-minio-31bf38666-amd64-en-day-minio-31bf38666-am
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-Client-Features-Package-multimedia \sim 31bf3856ad364e35 \sim amd 64 \sim end of the contraction of 
 US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Client-Features-Package-net \\ ^31bf3856ad364e35\\ ^{-}amd64\\ ^{-}end64\\ ^{e
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
redist-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
 shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
termsrv~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
US~6.2.9200.16384.cat
                                                                                   C:\Windows\Svstem32\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
00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim
US~6.2.9200.16384.cat
Opens: C: \windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\wicrosoft-Windows-Client-Features-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
US~6.2.9200.16384.cat
Opens:
                                                                                   C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                   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-
00C04FC295EE}\Microsoft-Windows-COM-MSMQ-package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Mindows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-admin-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295EE}\Microsoft-Windows-Common-Drivers-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-Common-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE \} \\ \ Microsoft-Windows-Common-Drivers-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3856ad364e35~amd64~enders-Package-ds~31bf3866ad364e35~amd64~enders-Package-ds~31bf3866ad364e35~amd64~enders-Package-ds~31bf3866ad364e36~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd64e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e366~amd66e3666~amd66e366~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e3666~amd66e36666~amd66e36666~amd66e366666~amd66e36666~amd66e36666~amd66e36666~amd66e36666~amd66e36666~amd66e36666~a
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
ds-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
\label{lem:condition} Opens: C: \windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-\windows-Common-Drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-Package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-package-minkernel-31bf3856ad364e35-amd64-ended-common-drivers-package-minkernel-31bf3856ad364-amd64-ended-common-drivers-package-minkernel-31bf3856ad364-amd64-ended-common-drivers-package-minkernel-31bf3856ad364-amd64-ended-common-drivers-package-minkernel-31bf3856ad364-amd64-ended-common-drivers-package-minkernel-31bf3856ad36-amd64-ended-common-drivers-package-minkernel-31bf3856-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-drivers-package-minkernel-31bf386ad36-amd64-ended-common-driver
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-Common-Drivers-Package-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D
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-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
 termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-vm~31bf3856ad364e35~amd64~en-
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
                                                                                          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-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 \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-1000 \\ \sim en-10
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Foundation-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          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:
 00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CommonFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \\ \verb|\Microsoft-Windows-CoreSystem-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3856ad364e35-amd64-en-Minio-Package-31bf3866ad364e35-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-en-Minio-Package-31bf3866ad364-amd64-amd64-en-Minio-Package-31bf3866ad364-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-a
 US~6.2.9200.16384.cat
                                                                                          C:\Windows\Svstem32\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-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
```

```
Opens
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-CoreSystem-Net-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364e35-amd64-en-Package-31bf3856ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf3866ad364-amd64-en-Package-31bf38666ad366-amd64-en-Package-31bf38666-amd66666-amd66666-amd6666-amd66666-amd6666-amd66666-amd66666-amd66666-amd66666-am
US~6.2.9200.16384.cat
\label{lem:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:copens:cop
                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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\} \land Microsoft-Windows-CoreSystem-Windows-Package \sim 31bf3856ad364e35 \sim amd 64 \sim end of the contraction of the cont
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-CoreSystem-WOW64-Mincore-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim endownormal \\ \sim endown
US~6.2.9200.16384.cat
                                                                                          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-
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Minkernel-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Net-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
      Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Net-
Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-CoreSystem-WOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-MOW64-Package \\ \sim amd64 \\ 
US~6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-
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-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Dedup-ChunkLibrary-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~endows-Dedup-ChunkLibrary-Package \\ ~31bf3856ad364e35 \\ ~amd64 \\ ~amd6
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-admin-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package
admin-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package~31bf3856ad364e35-amd64~en-
```

```
US~6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Editions-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package-31bf3856ad364e35-amd64~en-
 US~6.2.9200.16384.cat
       Opens:
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-FCI-Client-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
Opens:
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-FCI-Client-Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-Foundation-Package \\ \sim 31bf3856ad364e35 \\ \sim amd \\ 64 \\ \sim 6.2.9200.16384.cate \\ \sim 6.2.9200.0638.cate \\ \sim 6.2.9200.cate \\ \sim 6.2.9200.0638.cate \\ \sim 6.2.9200.0638.cate \\ \sim 6.2.9200.0638.cate \\ \sim 
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-
 admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 ODCO4FC295EE)\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-admin-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                          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-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-admin-31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
Opens:
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-admin-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-base~31bf3856ad364e35~amd64~en-
                                                                                                           C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE\} \land Microsoft-Windows-GroupPolicy-ClientTools-Package-com \sim 31bf3856ad364e35 \sim amd 64 \sim en-1000 colors of the colo
 US~6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 com-31bf3856ad364e35-amd64~-6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-drivers-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-drivers-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                        C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 enduser-31bf3856ad364e35-am664-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-GroupPolicy-ClientTools-Package enduser-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
 Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE}\windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295EE-00C04FC295E
 inetcore~31bf3856ad364e35-amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetcore-31bf3856ad364e35-amd64--6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 inetsrv-31bf3856ad364e35-am664-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 OOCO4FC295E}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetsrv-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \verb+\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio+ 31bf3856ad364e35+ amd 64-en-defined by the state of the sta
 US~6.2.9200.16384.cat
 Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE \\ | Microsoft-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Wind
 minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                          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-
      Opens:
  00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
        Opens:
                                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-GroupPolicy-ClientTools-Package-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Window
 printscan-31bf3856ad364e35-amd64-en-U5-6.2.9200.16384.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-endown-fine the control of th
  US~6.2.9200.16384.cat
                                                                                                           C:\Windows\Svstem32\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-
 OOC04FC295E5\Microsoft-Windows-GroupPolicy-ClientTools-Package-
termsrv-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
```

```
Opens
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODCO4FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
termsrv-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-windows-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
00C04FC295EE\} \\ Microsoft-Windows-GroupPolicy-ClientTools-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endormal \\ \sim endor
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Wicrosoft-Windows-HandwritingRecognizer-Package-31bf3856ad364e35-au
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
      Opens:
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-Help-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Windows-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Microsoft-Welp-ClientUA-Professional \\ \ MC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Identity-Foundation-Package~31bf3856ad364e35~an
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Add0n-2-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
      Opens:
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
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-IIS-WebServer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-Base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                                      C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
Base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-ImageBasedSetup-IE-Package-windows \sim 31bf3856ad364e35 \sim amd 64 \sim en-package-windows \sim 21bf3856ad364e35 \sim amd 64 \sim en-package-windows \sim 21bf3866ad364e35 \sim amd 64 \sim en-package-windows \sim 21bf3866ad364e36 \sim amd 64 \sim en-package-windows \sim 21bf3866ad364 \sim amd 64 \sim en-package-windows \sim 21bf3866ad364 \sim en-package-windows \sim 21bf3866ad364 \sim en-package-windows \sim 21bf3866ad364 \sim en-package-windows \sim en-package-windows \sim 21bf3866ad364 \sim en-package-windows \sim en-packa
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package-31bf3856ad364e35~amd64~en-US~10.0.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
                                                                                      C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C: \verb|Windows>System32| catroot| $F750E6C3-38EE-11D1-85E5-00C04FC295EE| \verb|Microsoft-Windows-InternetExplorer-Package-ua-31bf3856ad364e35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-amd64-35-am
US~6.2.9200.16384.cat
                                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                      C: \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-InternetExplorer-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExplorer-
Package-31bf3856ad364e35-amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Killbits-Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODCO4FC295EE}\Microsoft-Windows-Links-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE\} \\ Microsoft-Windows-Media-Format-Package-avcore~31bf3856ad364e35~amd64~en-defined by the control of the contro
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
windows-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Streaming-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-Media-Streaming-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-Media Center-Package-avcore ~31bf3856ad364e35 ~amd 64 ~endows-Media Center-Package-avcore ~amd 64 ~amd
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-
 avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                         C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE \} \\ Microsoft-Windows-Media Player-Package-avcore \\ ^{31bf3856ad364e35} \\ ^{amd64} \\ ^{en-package-avcore} \\ ^{31bf3856ad364e35} \\ ^{31bf386ad364e35} \\ ^{31bf386ad364} \\ ^{31
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-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\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \\ Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
    Opens:
                                                                         C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
Opens: C:\Windows\BobilePC-Client-Basic-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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-
US~6.2.9200.16384.cat
     Opens:
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
    Opens:
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                         C:\Windows\Svstem32\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\} \land Microsoft-Windows-Mobile PC-Client-SideShow-Package-ua \sim 31bf3856ad364e35 \sim amd 64 \sim en-control of the control of the contr
US~6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-MobilePC-Client-SideShow-Package-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Win
ua~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-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\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-admin~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
```

```
Opens
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\f750E6C3-38EE-11D1-85E5-
00C04FC295E}\Microsoft-Windows-Multilingual-Package-
drivers-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\f750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
ds-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-minkernel-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ Microsoft-Windows-Multilingual-Package-shell-31bf3856ad364e35-amd64-ended from the control of the control o
                                                       C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
shell-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
windows-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-
AutoNgenEnable.3.5~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-
NgenAssemblyExclusionClient-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Misc~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
\label{thm:condition} Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-M0F-120FC295EE}.
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04EC295EE}\Microsoft-Windows-NetEx-Shared-MOE-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
US~6.2.9200.16384.cat
Opens:
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODCO4FC295EE}\Microsoft-Windows-NetFx-Shared-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Client~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Extended~31bf3856ad364e35~amd64~-6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Typelibs~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-NetFx-Shared-WCF-
HttpActivation-31bf3856ad364e35-amd64--6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpNamespace~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
MsmqActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
PipeActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
TcpActivation-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
 TcpPortSharing~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                       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}\windows-NetFx-Shared-WPF-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-VCRedist-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Windows-Built-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx2-0C-Package~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-0C-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package-redist-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
```

```
Opens
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-1101-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-0C-Package-31bf3856ad364e35-amd64-en
US~6.2.9200.16384.cat
    Opens:
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx4-US-0C-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-1101-85E5-00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-0C-Package-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ParentalControls-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
OCCO4FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-PeerToPeer-Full-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-package 
US~6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\wirrosoft-Windows-PeerToPeer-Full-
Package=31bf3856ad364e35-am664~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Personalization-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-PlayToManager-Package \\ ^31bf3856ad364e35 \\ ^amd64 \\ ^a6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{E750E6C3-38EE-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-
    Opens
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-windows-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
Opens: C: \verb|Windows\System32| catroot\ \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ \verb|Microsoft-Windows-PowerShell-V2-Client-|
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE\} \land Microsoft-Windows-Presentation-Package \sim 31bf3856ad364e35 \sim amd 64 \sim end of the contraction of the contractio
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Presentation-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
Opens:
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Printing-Windows-Printing-Foundation-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-Package-31bf
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
 00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-LocalPrinting-Home-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
C:\windows\system32\catroot\
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-
Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens
```

```
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE}\Microsoft-Windows-PsuedoTool-HashIDSpy-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C: \verb|Windows| System32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE| \verb|Microsoft-Windows-RasCMAK-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat| catroot| 
Opens: C:\Windows\System32\Catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RasRip-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Redhawk-v1.0-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                        C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
UOLUH-L295E;\MICTOSOTT-WINDOWS-REMOTEDESKTOP-USERMODERPFOTOCOI-
Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
                                                       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
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens
00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RotMgr-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-
base-31bf3856ad364e35-amd64--6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        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-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                        C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-APPXLOB-Client
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-OCUR-
Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
\label{lem:opens:opens:c:windowsSystem32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\\ \label{lem:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:opens:
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-ProfessionalWMC-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ServicingBaseline-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-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-
00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Package-31bT385bad364e35-amd64--0.2.9200.1b384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-Wallpaper-Common-
Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
 Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-SKU-Foundation-Package-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D
 admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
 avcore-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-base~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C: \verb|Windows| System32| catroot| \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-SKU-Foundation-Package-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364e35-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-ended-com-31bf3856ad364-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd
 US~6.2.9200.16384.cat
                                                                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-drivers~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
 Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~en-databases-amount of the control of
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package
 ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-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~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~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
  US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
 enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-SKU-Foundation-Package-inetcore-31bf3856ad364e35-amd64-en-defendant and the control of the control 
 US~6.2.9200.16384.cat
 Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-SKU-Foundation-Package-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D
 00C04FC295EE \} \\ Microsoft-Windows-SKU-Foundation-Package-inetsrv-31bf3856ad364e35-amd64-en-defined by the control of the co
 US~6.2.9200.16384.cat
                                                                                                                                          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
                                                                                                                                         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-
  00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minio-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minio-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minkernel~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minkernel~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
 multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-net-31bf3856ad364e35-amd64-en-defined by the contraction of the cont
 US~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
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-printscan~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
 printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sdktools~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
          Opens
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-sdktools-31bf3856ad364e35-amd64--6.2.9200.16384.cat
 \label{lem:condition} Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-SKU-Foundation-Package-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e35-amd64-en-backage-shell-31bf3856ad364e36-amd64-en-backage-shell-31bf3856ad364e36-amd64-en-backage-shell-31bf3856ad364e36-amd64-en-backage-shell-31bf3856ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad364e36-amd64-en-backage-shell-31bf386ad366-amd64-en-backage-shell-31bf386ad366-amd64-en-backage-shell-31bf3
US~6.2.9200.16384.cat
Opens:
                                                                                                                                          C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-shell-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
                                                                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \verb+\Microsoft-Windows-SKU-Foundation-Package-sql-31bf3856ad364e35-amd64-en-defined by the statement of the sta
 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-
```

```
00C04FC295FF}\Microsoft-Windows-SKU-Foundation-Package-termsry~31bf3856ad364e35~amd64~en-
  US~6.2.9200.16384.cat
 Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-SKU-Foundation-Package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-package-pa
 termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE\} \\ \ Microsoft-Windows-SKU-Foundation-Package-ua~31bf3856ad364e35~amd64~en-decomposition and the second statement of the second stateme
  US~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
  ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows~31bf3856ad364e35~amd64~en-
 US~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-
        Opens:
  00C04FC295EE}\Microsoft-Windows-SKU-Foundation-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-

C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-SnippingTool-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim end 64 \\ \sim
 US~6.2.9200.16384.cat
 Opens: C: \windows\System 32\catroot\F750E6C3-38EE-11D1-85E5-00C04FC295EE\}\windows-SnippingTool-Package-31bf3856ad364e35-amd64~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package-31bf3856ad364e35-amd64~en-US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
 00C04FC295EE\} \\ \ Microsoft-Windows-SpeechRecognizer-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endown \\ \sim 100c04FC295EE \\ \sim 100c04FC29
  US~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
  00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e39
 US~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
00C04FC295EE}\Microsoft-Windows-5tickyNotes-Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-StorageService-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim 100c04FC295EE \\ \sim 100c04FC2
 US~6.2.9200.16384.cat
                                                                                                               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 \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim 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-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
 00C04FC295EE}\Microsoft-Windows-TabletPC-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \land Microsoft-Windows-TabletPC-Package \sim 31bf3856ad364e35 \sim amd 64 \sim 6.2.9200.16384. cather the state of the control of the con
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
 00C04FC295EE\} \land Microsoft-Windows-Telnet-Client-Package \sim 31bf3856ad364e35 \sim amd 64 \sim end of the contract of
 US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~en
US~6.2.9200.16384.cat
Opens:
                                                                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools
 Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-Terminal Services-Command Line Tools-Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
 Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider
Package-31bf3856ad364e35-amd64~6.2.9200.16384.cat
                                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
        Opens:
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~3lbf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
 00c04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~amd64~en-
  US~6.2.9200.16384.cat
                                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens
 00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
Opens: C.\Windows\systems2\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\oot\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\ood\\(\alpha\)\cat\o
```

```
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WindowsFoundation-LanguagePack-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
      Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-TroubleshootersPackage~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-
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
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Win0cr-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODC04FC295EE}\Microsoft-Windows-WinOur-Package-31bf3856ad364e35-amd64-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinSATMediaFiles-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-WMPNetworkSharingService-Package-31bf3856ad364e35-amd64-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007-end-2007
US~6.2.9200.16384.cat
Opens: C: \verb|Windows\System32| catroot\F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ |Microsoft-Windows-wMPNetworkSharingService-1000FC295EE \\ |Microsoft-Windows-wm-1000FC295EE \\ 
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE\} \land Microsoft-Windows-Xps-Foundation-Client-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-1000 \times 1000 \times 1
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\nt5.cat
       Opens
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\ntexe.cat
       Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\ntpe.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\ntph.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
00C04FC295EE}\oem0.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-AM-Default-Definitions-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
\label{eq:condition} $$00C04FC295EE}\windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat \\ Opens: 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
00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\windows-legacy-whql.cat
Opens: C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
                                                                                                 C:\Windows\Branding
C:\Windows\Branding\Basebrd
       Opens
       Opens
                                                                                                 C:\Windows\System32\en-US\sppsvc.exe.mui
C:\Windows\System32\sppobjs.dl1
C:\Windows\Branding\Basebrd\basebrd.dl1
       Opens:
       Opens:
        Opens:
       Opens:
                                                                                                 C:\Windows\Svstem32\wwapi.dll
                                                                                                          \Windows\System32\wscinterop.dll
        Opens:
       Opens:
                                                                                                 C:\Windows\System32\wscapi.dll
       Opens:
                                                                                                          \Windows\System32\wscui.cpl
                                                                                                 C:\Windows\System32\wscinterop.dll.123.Manifest
C:\Windows\System32\en-US\wscui.cpl.mui
       Opens:
       Opens:
       Opens:
                                                                                                 C:\Windows\System32\werconcpl.dll
C:\Windows\System32\framedynos.dll
       Opens
                                                                                                 C:\Windows\System32\wercplsupport.dll
C:\Windows\System32\msxml6.dll
       Opens:
       Opens:
                                                                                                  \begin{tabular}{ll} $C:\Windows\System32\msxml6r.dll \\ $C:\Windows\WER\ReportArchive. \end{tabular} \label{table:likelihood}
       Opens:
       Opens:
                                                                                                          \ProgramData\Microsoft\Windows\WER\ReportArchive \Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
       Opens
       Opens:
                                                                                                 C:\Windows\System32\hcproviders.dll
C:\Windows\System32\en-US\hcproviders.dll.mui
        Opens:
       Opens:
                                                                                                  C:\Program Files\Internet Explorer\ieproxy.dll
        Opens:
                                                                                                 C:\Windows\Svstem32\en-US\ActionCenter.dll.mui
       Opens:
                                                                                                          \Windows\System32\Actioncenter.dll.3.Manifest
        Opens:
       Opens:
Opens:
                                                                                                  C:\windows\system32\spp\store\data.dat \\ C:\windows\system32\spp\plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-signed\sppwinob-spp-plugin-manifests-
manifest-signed.xrm-ms
```

C:\Windows\System32\sppwinob.dll

Opens

```
Opens
                                                       C:\Windows\System32\netani32.dll
   Opens:
                                                       C:\Windows\System32\netutils.dll
   Opens:
                                                       C:\Windows\System32\srvcli.dll
C:\Windows\System32\wkscli.dll
   Opens:
                                                       C:\Windows\System32\dsrole.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
C:\Windows\System32\spp\store\data.dat.bak
   Opens:
   Opens:
                                                       C:\Windows\System32\en-US\KernelBase.dll.mui
C:\Windows\System32\taskschd.dll
   Opens:
   Opens:
                                                       C:\Windows\System32\sspicli.dll
C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
   Writes to:
1001\$915369118a4888a39e2f92dbd118adb3\@
Writes to: C:\$Recycle.Bin\$-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
                                                       C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
   Writes to:
    Writes to:
                                                       C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
                                                       C:\Windows\assembly\GAC_64\Desktop.ini
C:\Windows\ssembly\GAC_32\Desktop.ini
C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
   Writes to:
    Writes to:
   Writes to:
   Writes to:
                                                       C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
   Writes to:
Reads from:
                                                       C:\Windows\System32\spp\store\data.dat.tmp
C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
                                                       C:\Windows\SysWOW64\cmd.exe
C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
   Reads from:
   Reads from:
                                                       C:\$Recycle.Bin\S-1-5-18\$915369118a488a39e2f92dbd118adb3\@
C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
   Reads from:
   Reads from:
   Reads from:
                                                       C:\Windows\Prefetch\TASKHOST.EXE-CC5C42C1.pf
   Reads from:
C: \verb|Vars\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage\_1024\_768\_POS4.jpg| In the control of the co
   Reads from:
                                                       C:\Users\desktop.ini
                                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
   Reads from:
                                                       C:\Users\Admin\Desktop\desktop.ini
C:\Users\Public\desktop.ini
    Reads from:
   Reads from:
                                                       C:\Users\Public\Desktop\desktop.ini
                                                       C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
   Reads from:
   Reads from:
                                                       {\tt C:\Windows\System32\spp\store\data.dat}\\
                                                       C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
   Reads from:
manifest-signed.xrm-ms
  Reads from:
                                                       C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
manifest-signed.xrm-ms
                                                       C:\Windows\System32\spp\store\cache\cache.dat
   Reads from:
                                                       C:\Windows\System32\spp\store\tokens.dat
C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
   Reads from:
   Deletes:
                                                       C:\Windows\System32\spp\store\data.dat.tmp
```

Network Events

DNS query:	j.maxmind.com
DNS response:	j.maxmind.com ⇒ 127.0.0.1
Connects to:	127.0.0.1:80
Sends data to:	8.8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	206.254.253.254:16470
Sends data to:	190.254.253.254:16470
Sends data to:	180.254.253.254:16470
Sends data to:	135.254.253.254:16470
Sends data to:	115.254.253.254:16470
Sends data to:	88.254.253.254:16470
Sends data to:	87.254.253.254:16470
Sends data to:	71.254.253.254:16470
Sends data to:	243.253.253.254:16470
Sends data to:	241.253.253.254:16470
Sends data to:	240.253.253.254:16470
Sends data to:	213.253.253.254:16470
Sends data to:	212.253.253.254:16470
Sends data to:	201.253.253.254:16470
Sends data to:	190.253.253.254:16470
Sends data to:	24.125.167.254:16470
Sends data to:	200.85.163.252:16470
Sends data to:	76.123.113.252:16470
Sends data to:	75.179.58.251:16470
Sends data to:	188.24.139.250:16470
Sends data to:	67.169.22.247:16470
Sends data to:	24.91.128.246:16470
Sends data to:	65.190.35.245:16470
Sends data to:	76.29.170.239:16470
Sends data to:	5.13.167.239:16470
Sends data to:	82.131.125.232:16470
Sends data to:	68.37.72.231:16470
Sends data to:	219.106.83.230:16470
Sends data to:	68.61.232.228:16470
Sends data to:	76.107.98.5:16470
Sends data to: Sends data to:	69.199.239.225:16470 61.86.46.6:16470
Sends data to:	94.112.235.6:16470
Sends data to:	68.185.68.224:16470
Sends data to:	74.12.46.223:16470
Sends data to:	50.136.31.221:16470
Sends data to:	173.21.26.221:16470
Sends data to:	76.182.171.220:16470
Sends data to:	118.8.112.220:16470
Sends data to:	70.182.4.219:16470
Sends data to:	98.85.39.13:16470
Sends data to:	37.2.137.13:16470
Sends data to:	184.89.197.216:16470
Sends data to:	76.178.167.13:16470
Sends data to:	200.30.249.214:16470
Sends data to:	106.51.95.15:16470
Sends data to:	174.7.120.16:16470
Sends data to:	46.59.73.17:16470
Sends data to:	31.41.65.21:16470
Sends data to:	190.73.8.212:16470
Sends data to:	180.196.236.210:16470
Sends data to:	213.92.177.210:16470
Sends data to:	174.48.147.210:16470

Receives data from: 0.0.0.0:0

Opens key Opens key

Windows Registry Events

Creates key: HKCU\software\classes\clsid Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9} HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-Creates key 409d6c4515e9}\inprocser er32 Creates key: HKCU\software\microsoft\internet explorer\toolbar HKCU\software\microsoft\internet explorer\toolbar\shellbrowse Creates key Creates key HKLM\svstem\currentcontrolset\control\graphicsdrivers\connectivitv\ Creates key: HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity Creates key Creates key: $\label{thm:local} HKLM \system \current controls et\control \graphics drivers \configuration \$ Creates key: Creates key: HKCU\software\microsoft\windows\currer
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.106 HKCU\software\microsoft\windows\currentversion\action Creates key: center\checks\{e8433b72-HKCU\software\microsoft\windows\currentversion\action-5842-4d43-8645-bc2c35960837}.check.101 $\label{local-continuous} Creates key: \\ HKCU\software\microsoft\windows\currentversion\action center\checks\ee843b72-5842-4d43-8645-bc2c35960837\}.check.103$ Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100 Creates key: HKCU\software\microsoft\windows\current\ center\checks\{e8433b72-5842-4d43-8645-bc2c35960837},check.102 HKCU\software\microsoft\windows\currentversion\action Creates key: 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 Creates key HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101 Creates key: HKCU\software\microsoft\windows\cur center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0 HKCU\software\microsoft\windows\currentversion\action $\label{local-continuous} Creates \ key: \\ HKCU\ software\ microsoft\ windows\ current version\ action \\ center\ checks\ \{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc\}\ .\ check\ .\ 0$ $\label{thm:local-prop} $$HKCU\software\microsoft\windows\currentversion\startupnotify $$HKCU\software\microsoft\windows\currentversion\action $$$ Creates key: Creates key center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1\}.check.0
Creates key: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018} Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks 42fa-414c-b8aa-eee2c8202018}.check.100 Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\ 42fa-414c-b8aa-eee2c8202018}.check.101 Creates key HKCU\software\microsoft\windows\currentversion\action center\provider entlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881} Creates key HKCU\software\microsoft\windows\currentversion\action center\checks 4d2a-4d44-94bf-e0091898c881}.check.100 Creates key $\label{lem:creates} Creates key: $$ HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78\}}$ $\label{local-continuous} Creates key: \\ HKCU\software\microsoft\windows\currentversion\action center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78\}.check.101$ $\label{lem:creates} Creates \ key: $$ HKCU\software\microsoft\windows\currentvectors \equiv {$a5268b8e-7db5-465b-bab7-bdcda39a394a} $$$ Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a\}.check.100 Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}.check.800 Creates key: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023} Creates key: HKCU\software\microsoft\windows\current 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\currentver Creates key center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{3ff37a1c -a68d-4d6e-8c9b-f79e8b16c482}.check.100 HKCU\software\microsoft\windows\currentversion\action Creates key ventlog\{2374911b-b114-42fe-900d-54f95fee92e5} HKCU\software\microsoft\windows\currentversion\action center\provide Creates key: center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010 HKCU\software\microsoft\windows\currentversion\action Creates key: center\provide og\{aa4c798d-d91b-4b07-a013-787f5803d6fc} Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100 Creates key $\label{eq:hklmsystemwpa} \begin{tabular}{ll} HKLM\system\pa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34 \end{tabular}$ Creates key $\label{thm:hklm} HKLM \software \microsoft \windows \current version \run[windows defender] \\ HKLM \software \microsoft \wow 64$ Deletes value Opens key: Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key HKLM\system\currentcontrolset\control\safeboot\option Opens key HKLM\system\currentcontrolset\control\srp\gp\dll Opens key HKLM\softwar e\wow6432node\policies\microsoft\windows\safer\codeidentifiers HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens key $\label{thm:condition} \begin{tabular}{ll} HKCU \software \part \$ Opens key HKLM\system\currentcontrolset\control\nls\customlocale HKLM\system\currentcontrolset\control\nls\language Opens key Opens key HKLM\system\currentcontrolset\control\mui\uilanguages HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: Opens key HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings Opens key HKLM\software\policies\microsoft\mui\settings Opens key: $\label{thm:local-parameter} HKCU\control\ panel\desktop\muicached\machinelanguageconfiguration \\ HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration \\$ Opens key Opens key: Opens key HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration Opens key: Opens key: HKCU\control panel\desktop
HKCU\control panel\desktop\muicached $\label{thm:hklm} HKLM \software \subseteq \ wow 6432 node \subseteq \ microsoft \ mi$ Opens key

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the current version \end{tabular} approximately approxima$

```
Opens key:
                                                                                                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
       Opens key
                                                                                                              HKLM\software\microsoft\window
nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key: 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\windows
nt\currentversion\gre_initialize
                                                                                                              HKLM\software\wow6432node\microsoft\windows
       Opens key:
nt\currentversion\compatibility32
                                                                                                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
      Opens key:
compatibility
                                                                                                              HKLM\
       Opens key:
        Opens key:
                                                                                                              Opens key:
                                                                                                              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
        Opens key:
                                                                                                              HKLM\system\currentcontrolset\control\lsa
       Opens key:
 HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
       Opens key:
                                                                                                              HKLM\system\currentcontrolset\control\nls\extendedlocale
                                                                                                              HKLM\system\currentcontrolset\control\nls\sorting\ids
        Opens kev:
       Opens kev:
                                                                                                              HKLM\system\currentcontrolset\control\session manager
       Opens key:
                                                                                                              {\tt HKLM \ } system \verb|\  current control set \verb|\  control \verb|\  compression | \\
       Opens key:
                                                                                                              HKLM\software\policies\microsoft\sqmclient\windows
                                                                                                              HKLM\software\microsoft\sqmclient\windows
       Opens key:
                                                                                                              HKLM\system\currentcontrolset\services\winsock2\parameters
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
       Opens key:
       Opens key
       Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog\1e6c4482
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\00000005
       Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
        Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000000001
       Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
\label{thm:local_catalog} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MKL\begin{tabular
       Opens key:
\label{thm:local_catalog} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MKL\begin{tabular
       Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000000
       Opens kev:
Opens kev:
Opens kev:
\label{local-observation} HKLM \xspace \xspa
      Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
       Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000001
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000005
       Opens key:
Opens key:
                                                                                                              HKLM\software\microsoft\windows nt\currentversion\windows
       Opens key
HKLM \label{eq:hklm} Noftware \policies \microsoft \system certificates \noot \certificates \2bd63d28d7bcd0e251195aeb519243c13142ebc3 \noothing 
       Opens key:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus root \setminus certificates \setminus 2bd63d28d7bcd0e251195aeb519243c13142ebc3 \setminus root \setminus ro
Opens key: HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
                                                                                                              HKLM\system\currentcontrolset\services\winsock\parameters
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
       Opens key:
       Opens key:
                                                                                                              HKLM\system\currentcontrolset\services\winsock\setup migration\providers
       Opens key:
       Opens kev:
                                                                                                              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
       Opens kev:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus cryptography \setminus defaults \setminus provider \setminus microsoft \ base \ cryptographic \ base \ cryptograp
provider v1.0
       Opens key:
                                                                                                              HKLM\software\policies\microsoft\cryptography
                                                                                                             \label{thm:hklm} HKLM \software \mbox{\sc wow} 6432 node \mbox{\sc microsoft} \cryptography \sc filed additional to the context of the cont
       Opens kev:
       Opens key:
       Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
9a6f-135d9c6622cc}
       Opens key:
\label{thklm} HKLM \software \microsoft \windows \current version \explorer \shells ervice objects \ \{f56f6fdd-aa9d-4618-a949-c1b91af43b1a\}
                                                                                                              HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus windows \setminus current version \setminus runger = microsoft \setminus runger = mic
       Opens key:
       Opens kev:
                                                                                                              HKLM\software\wow6432node\microsoft\rpc
        Opens key:
                                                                                                              HKLM\system\currentcontrolset\control\computername\activecomputername
       Opens kev:
                                                                                                              HKLM\svstem\setup
                                                                                                               HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
        Opens key:
```

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010 Opens key:

HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32

HKLM\software\policies\microsoft\windows nt\rpc
HKLM\system\currentcontrolset\control\sqmservicelist

Opens key:

Opens key: Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\000000000000000
Opens key:
Opens key:
Opens key:
Opens key:
Opens key
\label{thm:mass} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MKL
     Opens key:
\label{thm:mass} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MKL
    Opens key:
HKLM\system\cu
                                              rentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries64\catalog.
     Opens key:
Opens kev:
Onens key
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\00000000000001
                                                                             HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
      Opens key:
                                                                             {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ offload \ \ \ )
                                                                             \label{thm:hklmsoftware} HKLM \software \mbox{\sc microsoft windows nt current version \sc profile list} \\ HKLM \software \mbox{\sc microsoft windows nt \c urrent version \sc profile list} \\ \label{thm:hklmsoftware}
     Opens key:
      Opens key:
     Opens key
                                                                             HKLM\system\currentcontrolset\control\session manager\environment
      Opens key:
                                                                              HKLM\software\microsoft\windows\currentversion
     Opens key
                                                                             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
      Opens key
                                                                              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
     Opens key:
                                                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKU\label{thm:local_hammon} HKU\label{thm:local_hammon} \begin{tabular}{ll} HKU\label{thm:local_hammon} \begin{tabular}{
shell folders
     Opens key:
                                                                             HKU\.default\environment
     Opens key
                                                                             HKU\.default\volatile environment
HKU\.default\volatile environment\0
     Opens key:
     Opens key
                                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
     Opens key:
                                                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the
options\rundll32.exe\perfoptions
                                                                             HKU\.default\software\microsoft\windows
     Opens key:
\label{lem:ntversion} $$ nt\currentversion\appcompatflags\ayers $$ Opens\ key: $$ HKLM\software\microsoft\windows $$ $$ $$
nt\currentversion\appcompatflags\custom\rundl132.exe
                                                                             HKLM\software\microsoft\windows\currentversion\sidebyside
     Opens key:
    Opens key:
                                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options
     Opens kev:
                                                                             HKU\.default\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                             HKU\.default\control
\label{thm:hkuldefault} HKU\.default\control\ panel\desktop\language\\ configuration\ HKU\.default\control\ panel\desktop\ 
     Opens key:
     Opens key
                                                                             HKU\.default\control panel\desktop\muicached

HKLM\system\currentcontrolset\control\error message instrument\

HKLM\system\currentcontrolset\control\error message instrument
     Opens key:
     Opens key
      Opens key
                                                                             HKLM\software\microsoft\windows nt\currentversion\gre initialize
     Opens key
                                                                             HKLM\software\microsoft\windows nt\currentversion\compatibility32
HKLM\software\microsoft\windows nt\currentversion\ime compatibility
      Opens key:
     Opens key
      Opens key
                                                                             {\tt HKLM \ } system \verb| current control \verb| set \verb| control \verb| cmf \verb| config
     Opens key
                                                                             HKLM\software\microsoft\rpc
                                                                              HKLM\system\currentcontrolset\services\bfe
      Opens key:
     Opens key
                                                                             HKLM\svstem\currentcontrolset\services\bfe\startoverride
                                                                              HKLM\system\currentcontrolset\services\aelookupsvc
      Opens key:
     Opens key
                                                                             HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
     Opens key:
                                                                              HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
     Opens key:
Opens key:
                                                                             \label{thm:local} HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\normaliset\services\alg
                                                                             HKLM\system\currentcontrolset\services\alg\triggerinfo HKLM\system\currentcontrolset\services\alluserinstallagent
     Opens key
     Opens key
     Opens key:
Opens key:
                                                                             Opens key
     Opens key
      Opens key
                                                                             HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
     Opens key
                                                                              HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
      Opens key:
     Opens key
                                                                             HKLM\system\currentcontrolset\services\appinfo
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\appinfo\triggerinfo
     Opens key
                                                                             HKLM\system\currentcontrolset\services\appmgmt
                                                                              HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
      Opens key:
     Opens key
                                                                             HKLM\system\currentcontrolset\services\audioendpointbuilder
     Opens key:
                                                                              {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  audioend point builder \verb|\  trigger info
     Opens key:
Opens key:
                                                                             HKLM\system\currentcontrolset\services\audiosrv
                                                                             HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
     Opens key
                                                                             HKLM\system\currentcontrolset\services\axinstsv
HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
     Opens key
                                                                             HKLM\system\currentcontrolset\services\bdesvc
HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
     Opens key
     Opens key:
Opens key:
                                                                             HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0 HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
     Opens key:
                                                                             {\tt HKLM \ } system \verb| current control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| bfe \verb| trigger info excest the control set \verb| services \verb| s
                                                                             HKLM\svstem\currentcontrolset\services\bits
     Opens key
      Opens key:
                                                                              {\tt HKLM \controlset \control
     Opens key
                                                                             HKLM\svstem\currentcontrolset\services\brokerinfrastructure
                                                                              HKLM\system\currentcontrolset\services\brokerinfrastructure\triggerinfo
      Opens key:
     Opens kev:
                                                                             HKLM\svstem\currentcontrolset\services\browser
                                                                              HKLM\system\currentcontrolset\services\browser\triggerinfo
      Opens key:
     Opens key
                                                                             HKLM\system\currentcontrolset\services\browser\triggerinfo\0
                                                                              HKLM\system\currentcontrolset\services\browser\triggerinfo\1
      Opens key
      Opens key
                                                                             HKLM\system\currentcontrolset\services\browser\triggerinfo\2
      Opens key
                                                                             HKLM\system\currentcontrolset\services\browser\startoverride
```

```
Opens key
                                             HKLM\system\currentcontrolset\services\bthserv
   Opens key:
                                              HKLM\system\currentcontrolset\services\bthserv\triggerinfo
   Opens key
                                             HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
                                              HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
   Opens key:
   Opens key
                                             Opens key
   Opens key:
Opens key:
                                             HKLM\system\currentcontrolset\services\comsysapp
HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
   Opens key
                                             HKLM\system\currentcontrolset\services\cryptsvc
HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo
   Opens key
                                             HKLM\system\currentcontrolset\services\cscservice
HKLM\system\currentcontrolset\services\cscservice\triggerinfo
   Opens key
   Opens key
   Opens key:
                                             HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0
                                             HKLM\system\currentcontrolset\services\cscservice\triggerinfo\1
   Opens key
   Opens key:
                                             HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
   Opens key
                      e\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
                                             Opens key:
   Opens key:
   Opens key
                                             \label{thm:local_hammon_hammon} HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
   Opens key:
                                             \label{thm:local-ham} HKLM \software \microsoft \telemetry client \sample store \sqm \windows \ HKLM \software \microsoft \telemetry client \sample store \sqm \
   Opens key
   Opens key:
   Opens key
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
   Opens key:
                                              HKLM\system\currentcontrolset\services\dcomlaunch
                                             HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo
   Opens key:
   Opens key:
                                              HKLM\system\currentcontrolset\services\defragsvc
                                             HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
   Opens key
   Opens key:
                                              HKLM\system\currentcontrolset\services\deviceassociationservice
   Opens key
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo
   Opens kev:
\label{thm:mass} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular}
Opens key: HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\2
   Opens key:
                                             HKLM\system\currentcontrolset\services\deviceinstall
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo
   Opens key
   Opens key:
                                             HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0
   Opens key
                                             HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1
   Opens key:
                                              HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\2
   Opens key
                                             HKLM\system\currentcontrolset\services\dhcp
   Opens key:
                                              HKLM\system\currentcontrolset\services\dhcp\triggerinfo
   Opens key
                                             HKLM\svstem\currentcontrolset\services\dnscache
   Opens key
                                              HKLM\system\currentcontrolset\services\dnscache\triggerinfo
   Opens key
                                             HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
   Opens key:
                                              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
   Opens key
                                             HKLM\system\currentcontrolset\services\dnscache\startoverride
   Opens key:
                                              HKLM\system\currentcontrolset\services\dot3svc
   Opens key
                                             HKLM\system\currentcontrolset\services\dot3svc\triggerinfo
   Opens key:
                                              HKLM\system\currentcontrolset\services\dps
                                             HKLM\system\currentcontrolset\services\dps\triggerinfo HKLM\system\currentcontrolset\services\dsmsvc
   Opens key
   Opens key
                                             HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0
   Opens key
   Opens key
   Opens key
                                              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\1
                                             HKLM\system\currentcontrolset\services\eaphost
   Opens key
                                             HKLM\system\currentcontrolset\services\eaphost\triggerinfo
   Opens key
   Opens key
   Opens key
                                              HKLM\svstem\currentcontrolset\services\efs\triggerinfo\0
   Opens key
                                              HKLM\system\currentcontrolset\services\efs\triggerinfo\1
   Opens key:
                                             HKLM\system\currentcontrolset\services\eventlog
   Opens key
                                              HKLM\system\currentcontrolset\services\eventlog\triggerinfo
   Opens key
   Opens key
                                             HKLM\system\currentcontrolset\services\eventsystem
   Opens key:
                                              HKLM\system\currentcontrolset\services\eventsystem\triggerinfo
   Opens key:
Opens key:
                                             \label{thm:hklmsystem} HKLM \ system \ current controls et services \ fax \ HKLM \ system \ current controls et services \ fax \ trigger in formal \ fax \
                                             HKLM\system\currentcontrolset\services\fdphost
HKLM\system\currentcontrolset\services\fdphost\triggerinfo
   Opens key
   Opens key
   Opens key
                                             HKLM\system\currentcontrolset\services\fdrespub
HKLM\system\currentcontrolset\services\fdrespub\triggerinfo
                                             HKLM\system\currentcontrolset\services\fhsvc
HKLM\system\currentcontrolset\services\fhsvc\triggerinfo
   Opens key
   Opens key
   Opens key
                                             HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1
   Opens key
                                              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\2
   Opens key:
   Opens key
                                             HKLM\svstem\currentcontrolset\services\fontcache
   Opens key
                                              HKLM\system\currentcontrolset\services\fontcache\triggerinfo
   Opens key
                                             HKLM\svstem\currentcontrolset\services\fontcache3.0.0.0
                                              HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo
   Opens key:
   Opens key
                                             HKLM\system\currentcontrolset\services\gpsvc
   Opens key:
                                              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
   Opens key:
Opens key:
                                             HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\1
   Opens key
                                             HKLM\system\currentcontrolset\services\hidserv
HKLM\system\currentcontrolset\services\hidserv\triggerinfo
                                             HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0 HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1
   Opens key
   Opens key
   Opens key:
Opens key:
                                             HKLM\system\currentcontrolset\services\hkmsvc
HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
   Opens key:
                                              HKLM\system\currentcontrolset\services\homegrouplistene
                                             HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
   Opens key
   Opens key
                                              HKLM\system\currentcontrolset\services\homegroupprovider
                                             {\tt HKLM \ } \textbf{System \ } \textbf{Current control set \ } \textbf{Services \ } \textbf{homegroup provider \ } \textbf{Trigger in fo}
   Opens key
                                              HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0
   Opens key:
   Opens key
                                             HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\1
                                              HKLM\system\currentcontrolset\services\ikeext
   Opens key:
   Opens key
                                             HKLM\system\currentcontrolset\services\ikeext\triggerinfo
   Opens key:
                                              HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
   Opens key
                                             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1
   Opens key
                                              HKLM\system\currentcontrolset\services\ikeext\startoverride
```

```
Opens key
                                                                       HKLM\system\currentcontrolset\services\ivmservice
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\keyiso
                                                                       \label{thm:local_ham} $$HKLM\system\current control set\services\key is o\trigger in fo HKLM\system\current control set\services\key is o\trigger in fo \0 $$
     Opens key
     Opens key:
    Opens key
                                                                       HKLM\system\currentcontrolset\services\keyiso\triggerinfo\1 HKLM\system\currentcontrolset\services\ktmrm
     Opens key
    Opens key
Opens key
                                                                       \label{thm:local-ham} HKLM\system\currentcontrolset\services\ktmrm\triggerinfo+HKLM\system\currentcontrolset\services\ktmrm\triggerinfo+O
    Opens key
                                                                       HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1 HKLM\system\currentcontrolset\services\lanmanserver
    Opens key
                                                                       \label{thm:local_hammans} HKLM \system \current controlset \services \lammans erver \trigger in four hKLM \system \current controlset \services \lamman \system \current \system \sy
     Opens key
    Opens key
     Opens key
                                                                       {\it HKLM} \ 's y stem \ 'current control set \ 's ervices \ 'lanman work station \ 'trigger in footbase \ 's ervices' \ 's ervi
                                                                       HKLM\system\currentcontrolset\services\lltdsvc
    Opens key
      Opens key
                                                                        Opens key
                                                                       HKLM\system\currentcontrolset\services\lmhosts
     Opens key:
                                                                        Opens key
                                                                       HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0
     Opens key
                                                                        HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1
    Opens key
                                                                       HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2 HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\3
     Opens key:
     Opens key
                                                                       HKLM\svstem\currentcontrolset\services\lsm
                                                                        HKLM\system\currentcontrolset\services\lsm\triggerinfo
     Opens key:
    Opens key
                                                                       HKLM\svstem\currentcontrolset\services\mmcss
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\mmcss\triggerinfo
    Opens key:
Opens key:
                                                                       HKLM\system\currentcontrolset\services\msdtc
HKLM\system\currentcontrolset\services\msdtc\triggerinfo
                                                                       HKLM\system\currentcontrolset\services\msiscsi
HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
    Opens key
    Opens key
     Opens key
                                                                       HKLM\system\currentcontrolset\services\msiserver
                                                                       HKLM\system\currentcontrolset\services\msiserver\triggerinfo
    Opens key
                                                                        HKLM\system\currentcontrolset\services\napagent
      Opens key:
     Opens key
                                                                       HKLM\system\currentcontrolset\services\napagent\triggerinfo
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\ncasvc
    Opens key
                                                                       HKLM\system\currentcontrolset\services\ncasyc\triggerinfo
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0
     Opens key
                                                                       HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1
     Opens key
                                                                        HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2
    Opens key
                                                                       HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\3
                                                                        HKLM\system\currentcontrolset\services\ncdautosetup
     Opens key:
                                                                       Opens key
     Opens key:
                                                                       HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\1
HKLM\system\currentcontrolset\services\netlogon
    Opens key
    Opens key
     Opens key
                                                                       HKLM\system\currentcontrolset\services\netlogon\triggerinfo
    Opens key
     Opens key
                                                                        HKLM\system\currentcontrolset\services\netman\triggerinfo
     Opens key
                                                                       HKLM\system\currentcontrolset\services\netprofm
      Opens key
                                                                        Opens key
                                                                       HKLM\system\currentcontrolset\services\nettcpportsharing
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo
                                                                       HKLM\svstem\currentcontrolset\services\nlasvc
     Opens key
     Opens key
                                                                        HKLM\system\currentcontrolset\services\nlasvc\triggerinfo
    Opens key
                                                                       HKLM\svstem\currentcontrolset\services\nsi
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\nsi\triggerinfo
     Opens key
                                                                       HKLM\system\currentcontrolset\services\ose
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\ose\triggerinfo
    Opens key
                                                                       HKLM\svstem\currentcontrolset\services\p2pimsv
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
                                                                       HKLM\system\currentcontrolset\services\p2psvc
HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
     Opens key
    Opens key
                                                                       HKLM\system\currentcontrolset\services\pcasvc
HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
    Opens key
    Opens key
     Opens key
                                                                        HKLM\system\currentcontrolset\services\peerdistsvo
                                                                       HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo
    Opens key
                                                                       HKLM\system\currentcontrolset\services\perfhost
HKLM\system\currentcontrolset\services\perfhost\triggerinfo
     Opens key
     Opens key
     Opens key
                                                                        HKLM\system\currentcontrolset\services\pla
                                                                       HKLM\svstem\currentcontrolset\services\pla\triggerinfo
    Opens key
                                                                        HKLM\system\currentcontrolset\services\plugplay
     Opens key:
                                                                       \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\plugplay\triggerinfo} $$HKLM\system\currentcontrolset\services\pnrpautoreg $$
     Opens key
     Opens key
    Opens key
                                                                       HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\pnrpsvc
     Opens key
                                                                       \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\prizes\
     Opens key:
                                                                       HKLM\system\currentcontrolset\services\policyagent\triggerinfo
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
    Opens key
     Opens key
                                                                       HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1 HKLM\system\currentcontrolset\services\policyagent\startoverride
     Opens key
     Opens key:
    Opens key
                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
    Opens key:
                                                                        {\tt HKLM \control \c
                                                                       HKLM\system\currentcontrolset\control\session manager\appcompatibility
     Opens key
                                                                        HKLM\software\wow6432node\policies\microsoft\windows\appcompat
     Opens key
     Opens key
                                                                       HKLM\software\policies\microsoft\windows\appcompat
      Opens key
                                                                        HKCU\software\microsoft\windows nt\currentversion
    Opens key
                                                                       HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
     Opens key
                                                                        HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
    Opens key:
                                                                       HKLM\software\wow6432node\microsoft\windows
\verb|nt\currentversion\appcompatflags\custom\cmd.exe|
    Opens key:
                                                                       HKLM\system\currentcontrolset\services\power
    Opens key:
Opens key:
                                                                       HKLM\system\currentcontrolset\services\power\triggerinfo HKLM\system\currentcontrolset\services\printnotify
                                                                       \label{thm:local-ham} HKLM \system \current control set \services \print notify \trigger in formal knowledge \current version \explorer \shell folders \end{substitute}
    Opens key
     Opens key
                                                                       \label{thm:loss} HKLM \software \microsoft \windows nt \current version \approximately approximately approximate
     Opens key
    Opens key
nt\currentversion\appcompatflags\custom\cmd.exe
                                                                       HKLM\svstem\currentcontrolset\services\profsvc
    Opens kev:
     Opens key:
                                                                        {\tt HKLM \ } system \verb| current control set \verb| services \verb| prof svc \verb| trigger info
    Opens key
                                                                       HKLM\svstem\currentcontrolset\services\gwave
                                                                        HKLM\system\currentcontrolset\services\qwave\triggerinfo
     Opens key:
     Opens key
                                                                       HKLM\system\currentcontrolset\services\rasauto
                                                                        HKLM\system\currentcontrolset\services\rasauto\triggerinfo
     Opens key:
    Opens key
                                                                       HKLM\system\currentcontrolset\services\rasman
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\rasman\triggerinfo
     Opens key
                                                                       HKLM\system\currentcontrolset\services\remoteaccess
     Opens key
                                                                        HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo
```

```
Opens key
                                                                       HKLM\system\currentcontrolset\services\remoteregistry
                                                                        HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo
     Opens key:
                                                                       HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0 HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\1
     Opens key
     Opens key:
    Opens key
                                                                       Opens key
    Opens key:
Opens key:
                                                                       HKLM\system\currentcontrolset\services\rpclocator HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
    Opens key
                                                                       HKLM\system\currentcontrolset\services\rpcss
HKLM\system\currentcontrolset\services\rpcss\triggerinfo
     Opens key
Opens key:
options\conhost.exe
                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
                                                                       HKLM\system\currentcontrolset\services\samss
    Opens key
                                                                       HKLM\system\currentcontrolset\services\samss\triggerinfo
     Opens key:
      Opens key
                                                                        HKLM\system\currentcontrolset\services\scardsvr
                                                                       HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
    Opens key
     Opens key:
                                                                        Opens key
                                                                       HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\2
    Opens key:
Opens key:
                                                                       HKLM\system\currentcontrolset\services\schedule
                                                                        HKLM\system\currentcontrolset\services\schedule\triggerinfo
     Opens key
                                                                       HKLM\system\currentcontrolset\services\scpolicysvc
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo
    Opens key
                                                                       HKLM\svstem\currentcontrolset\services\sdrsvc
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo
    Opens key:
Opens key:
                                                                       HKLM\software\microsoft\ole
HKLM\software\microsoft\ole\tracing
                                                                       HKLM\software\microsoft\oleaut
HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
    Opens key
    Opens key
                                                                       HKLM\software\microsoft\windows nt\currentversion\console\fullscreen HKLM\system\currentcontrolset\services\seclogon
     Opens key
    Opens key
                                                                        HKLM\system\currentcontrolset\services\seclogon\triggerinfo
      Opens key:
     Opens key
                                                                       HKLM\system\currentcontrolset\services\sens
                                                                        HKLM\system\currentcontrolset\services\sens\triggerinfo
     Opens key:
    Opens key
                                                                       HKCU\console
     Opens key:
     Opens key
                                                                       HKLM\system\currentcontrolset\services\sensrsvc
     Opens key
                                                                        HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
    Opens key
                                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
                                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2
     Opens key
     Opens key:
                                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\3
                                                                       HKLM\system\currentcontrolset\services\sessionenv
HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
    Opens key
    Opens key
     Opens key
                                                                       HKLM\system\currentcontrolset\services\shellhwdetection
HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
    Opens key
     Opens key
                                                                        HKLM\system\currentcontrolset\services\snmptrap
     Opens key
                                                                       HKLM\system\currentcontrolset\services\snmptrap\triggerinfo
      Opens key
                                                                        HKLM\system\currentcontrolset\services\spooler
                                                                       HKLM\system\currentcontrolset\services\spooler\triggerinfo
    Opens key
                                                                       HKCU\console\%systemroot%_system32\cmd.exe
HKCU\console\%systemroot%\system32\cmd.exe
HKLM\system\currentcontrolset\services\sppsvc
     Opens key:
     Opens key
     Opens key
                                                                       \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\sprsvc\triggerinfo-00. The local controlset\services\sprsvc\triggerinfo-00. The local controlset\sprsvc\triggerinfo-00. 
    Opens key
     Opens key:
     Opens key
                                                                       \label{thm:local} HKLM\system\currentcontrolset\services\sproxc\triggerinfo\normalised\currentcontrolset\control\normalised\currentcontrol\normalised\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\curren
     Opens key:
    Opens key
                                                                       HKLM\svstem\currentcontrolset\control\nls\locale\alternate sorts
                                                                        HKLM\system\currentcontrolset\control\nls\language groups
     Opens key:
                                                                       HKLM\system\currentcontrolset\services\ssdpsrv
HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
     Opens key
    Opens key
                                                                       HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
    Opens key
    Opens key
     Opens key
                                                                        HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo
                                                                       HKLM\system\currentcontrolset\services\stisvc
    Opens key
                                                                       HKLM\system\currentcontrolset\services\stisvc\triggerinfo
HKLM\system\currentcontrolset\services\storsvc
     Opens key
     Opens key
     Opens key
                                                                        {\tt HKLM \colored \c
                                                                       HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0
    Opens key
```

HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1 Opens key: Opens key HKLM\svstem\currentcontrolset\services\svsvc

HKLM\system\currentcontrolset\services\svsvc\triggerinfo Opens key:

Opens key HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0 Opens key: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\1 Opens key: Opens key: HKLM\system\currentcontrolset\services\swprv
HKLM\system\currentcontrolset\services\swprv\triggerinfo

HKLM\system\currentcontrolset\services\sysmain
HKLM\system\currentcontrolset\services\sysmain\triggerinfo Opens key Opens key Opens key HKLM\system\currentcontrolset\services\systemeventsbroker HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo

 $HKLM \system \current control set \services \system events broker \trigger in fold HKLM \system \current control set \services \system events broker \trigger in fold \system \syste$ Opens key Opens key Opens key HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\2 HKLM\system\currentcontrolset\services\tabletinputservice Opens key

Opens key: $\label{thm:hklm:system} \\ \textbf{HKLM} \\ \textbf{System: current control set: services: table tinput service: trigger information of the system of the$ Opens key HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0 Opens key HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1

Opens key HKLM\system\currentcontrolset\services\tapisrv

HKLM\system\currentcontrolset\services\tapisrv\triggerinfo Opens key: Opens key HKLM\system\currentcontrolset\services\termservice Opens key: HKLM\system\currentcontrolset\services\termservice\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\themes HKLM\system\currentcontrolset\services\themes\triggerinfo

Opens key HKLM\system\currentcontrolset\services\threadorder HKLM\system\currentcontrolset\services\threadorder\triggerinfo HKLM\system\currentcontrolset\services\timebroker HKLM\system\currentcontrolset\services\timebroker\triggerinfo Opens key Opens key Opens key: Opens key:

HKLM\system\currentcontrolset\services\timebroker\triggerinfo\2 HKLM\system\currentcontrolset\services\tlntsvr Opens key: Opens key Opens key ${\tt HKLM \colored \c$

Opens key HKLM\svstem\currentcontrolset\services\trkwks HKLM\system\currentcontrolset\services\trkwks\triggerinfo Opens key: Opens key HKLM\svstem\currentcontrolset\services\trustedinstaller

HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo Opens key:

Opens key HKLM\system\currentcontrolset\services\ui0detect

Opens key: HKLM\system\currentcontrolset\services\uiOdetect\triggerinfo Opens key HKLM\system\currentcontrolset\services\umrdpservice Opens key HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo

```
Opens key
                                                  HKLM\system\currentcontrolset\services\upnphost
Opens key:
                                                  HKLM\system\currentcontrolset\services\upnphost\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\vaultsvc
                                                  HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\vds
HKLM\system\currentcontrolset\services\vds\triggerinfo
Opens key
Opens key
Opens key
                                                  \label{thm:local_ham} HKLM \system \current controlset \services \v micheart beat \system \current controlset \services \v micheart beat \trigger in formal \system 
Opens key
                                                  HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0
HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\1
Opens key
                                                  HKLM\system\currentcontrolset\services\vmickvpexchange
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo
Opens key
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\1
Opens key
 Opens key
                                                  HKLM\system\currentcontrolset\services\vmicrdv
                                                  HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo
Opens key
 Opens key:
                                                  Opens key
                                                  HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\1
Opens key
                                                  HKLM\system\currentcontrolset\services\vmicshutdown
Opens key
                                                  HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0
Opens key:
Opens key
                                                  HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\1
                                                  HKLM\system\currentcontrolset\services\vmictimesync
Opens key
Opens key
                                                  {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  vmictimes ync \verb|\  trigger info
Opens key:
                                                  HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0
Opens key:
Opens key:
                                                  HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\1
HKLM\system\currentcontrolset\services\vmicvss
                                                  HKLM\system\currentcontrolset\services\vmicvss\triggerinfo HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0
Opens key
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\1
                                                  HKLM\system\currentcontrolset\services\vss
Opens key
                                                  HKLM\system\currentcontrolset\services\vss\triggerinfo
 Opens key:
Opens key
                                                  HKLM\system\currentcontrolset\services\w32time
Opens key
                                                  HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
Opens key:
                                                  HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key
                                                  HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
                                                  HKLM\system\currentcontrolset\services\wbengine
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wbengine\triggerinfo
Opens key:
                                                  HKLM\system\currentcontrolset\services\wbiosrvc
                                                  HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
Opens key
Opens key:
                                                  HKLM\system\currentcontrolset\services\wcmsvc
                                                  HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0
Opens key
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\1 HKLM\system\currentcontrolset\services\wcncsvc
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\wcspluginservice
 Opens key
                                                  HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\wdiservicehost
Opens key:
                                                  HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
                                                  HKLM\svstem\currentcontrolset\services\wdisvstemhost
Opens key
 Opens key
                                                  HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
Opens key
                                                  HKLM\svstem\currentcontrolset\services\webclient
Opens key:
                                                  HKLM\system\currentcontrolset\services\webclient\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
Opens key
                                                  HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
Opens key
                                                  HKLM\system\currentcontrolset\services\wecsvc
                                                  HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\wercplsupport
HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
Opens key
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wersvc
HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
                                                  HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key
                                                  HKLM\system\currentcontrolset\services\wiarpc
HKLM\system\currentcontrolset\services\wiarpc\triggerinfo
Opens key
Opens key
Opens key
                                                  {\tt HKLM \ } system \verb| current control set \verb| services \verb| windefend | \\
                                                  HKLM\system\currentcontrolset\services\windefend\triggerinfo
Opens key
                                                  HKLM\system\currentcontrolset\services\windefend\triggerinfo\0
Opens key:
Opens key
                                                  HKLM\system\currentcontrolset\services\windefend\triggerinfo\1
                                                  HKLM\system\currentcontrolset\services\winhttpautoproxysvo
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
Opens key:
                                                  HKLM\system\currentcontrolset\services\winmgmt
Opens key:
Opens key:
                                                  \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\winnmgmt\triggerinfo} $$HKLM\system\currentcontrolset\services\winrm $$
                                                  HKLM\system\currentcontrolset\services\winrm\triggerinfo HKLM\system\currentcontrolset\services\wlansvc
Opens key
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wlansvc\triggerinfo HKLM\system\currentcontrolset\services\wlidsvc
                                                  \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo-00. The local controlset\services\wlidsvc\triggerinfo-00. The local controlset\services\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wlines\wli
Opens key
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1
HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\2
Opens key
                                                  HKLM\system\currentcontrolset\services\wmiapsrv
Opens key:
                                                  HKLM\svstem\currentcontrolset\services\wmiapsrv\triggerinfo
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wmpnetworksvo
Opens key
                                                  HKLM\svstem\currentcontrolset\services\wmpnetworksvc\triggerinfo
                                                  HKLM\system\currentcontrolset\services\wpcsvc
Opens key:
Opens key
                                                  {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ wpcsvc \verb|\ triggerinfo | \\
Opens key:
                                                  HKLM\system\currentcontrolset\services\wpdbusenum
Opens key:
Opens key:
                                                  {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  wpdbusenum \verb|\  trigger info
                                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
Opens key
                                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1 HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
                                                  \label{thm:local-problem} HKLM \system \current controls et\services \wpdbusenum \trigger in fo\ 4 HKLM \system \current controls et\services \wpdbusenum \trigger in fo\ 4 HKLM \system \current \current \system \system \current \system 
Opens key
Opens key
                                                  Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wsearch\triggerinfo
Opens key:
Opens key
Opens key
                                                  HKLM\system\currentcontrolset\services\wsservice\triggerinfo
Opens key
                                                  HKLM\svstem\currentcontrolset\services\wsservice\triggerinfo\0
                                                  HKLM\system\currentcontrolset\services\wsservice\triggerinfo\1
Opens key:
Opens key
                                                  HKLM\svstem\currentcontrolset\services\wuauserv
                                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
Opens key:
Opens key
                                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0
Opens key:
                                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1
Opens key
                                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\2
Opens key
                                                  HKLM\system\currentcontrolset\services\wudfsvc
```

```
Opens key
                                  HKLM\system\currentcontrolset\services\wudfsyc\triggerinfo
  Opens key:
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
  Opens key
                                  HKLM\system\currentcontrolset\services\wwansvc
  Opens key:
  Opens key
                                  Opens key
Opens key: HKLM\softwar
1923240461-1905901954-2556564120-1001
                                  Opens key:
                                  HKU\s-1-5-21-1923240461-1905901954-2556564120
1001\software\microsoft\windows\currentversion\explorer\user shell folders
  Opens key:
                                  HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\environment
                                  HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\volatile environment
  Opens key
  Opens key
                                  HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\volatile
environment\0
  Opens key:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\taskhost.exe
                                   \label{lem:hklm} \verb+KLM\+ system \verb+ current control set \verb+ control + session manager \verb+ quota system \verb+ s-1-session manager \verb+ quota system manager \verb+ quota system manager \verb+ quota system manager \verb+ quota system manager man
5-21-1923240461-1905901954-2556564120-1001
                                  HKLM\software\microsoft\windows
  Opens key:
nt\currentve
                                  patflags\custom\taskhost.exe
  Opens key:
                                  HKCU\software\classes\
  Opens key
                                  HKCU\software\classes\appid\taskhost.exe
  Opens key:
                                  HKCR\appid\taskhost.exe
  Opens key
                                  HKCU\software\microsoft\windows\currentversion\directmanipulation
                                  HKLM\software\microsoft\com3
  Opens key
  Opens key
                                  HKLM\software\microsoft\windowsruntime\clsid
                                  HKLM\software\microsoft\windowsruntime\clsid\{900be39d-6be8-461a-bc4d-
  Opens key
b0fa71f5ecb1)
                                  HKCR\activatableclasses\clsid
  Opens key:
                                  HKCR\activatableclasses\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
  Opens key
  Opens key
                                   HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
   Opens key
  Opens key
                                  HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\treatas
  Opens key:
                                  HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\treatas
                                  HKCU\software\classes\clsid\{900be39d-6be8
   Opens key
b0fa71f5ecb1}\inprocserver32
  Opens key:
                                  HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprocserver32
  Opens key
                                  HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d
b0fa71f5ecb1}\inprochandler32
  Opens kev:
                                  HKCR\clsid\{900he39d-6he8-461a-hc4d-h0fa71f5ech1}\inprochandler32
                                  HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-
  Opens key
b0fa71f5ecb1}\inprochandler
                                  HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprochandler
  Opens key:
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
  Opens key
a37a-4f91-bdba
                    -fbb98fe804bf}
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8
                      3670ed91517}
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
393e-41c3-9885
                          :5a701926}
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
                     4b6b83dbf476}
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
fd02-4b82-a0a5-783266e430ab}
  Opens key:
                                  HKI M\
                                                         entcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
5780-49de-9eb5-8d53a51fd146}
Opens key:
86f7-41a4-b655
                                  HKI M\s
                                                     urrentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
                    bee3f2adef46}
                                  HKLM\
  Opens key
                                                          entcontrolset\control\wdi\diagnosticmodules\{5ee64afb
398d-4edb-af71-3b830219abf7}
                                  HKI M\
  Opens key:
                                                                ontrolset\control\wdi\diagnosticmodules\{63e0d0f7-
ac2f-493b-a7f2-2f3ccdb66fca}
Opens key: HKL
6c5b-43bb-860b-d47ae85242b1}
                                  HKLM
                                                                ntrolset\control\wdi\diagnosticmodules\{67f1ec80-
                                  HKLM\sy
  Opens key:
                                                          entcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b-d429828bea2e3
                                  HKLM\sy
                                                       rentcontrolset\control\wdi\diagnosticmodules\{7a54f16f
a73a-4258-ba46-a1e998a6aa74}
                                             stem\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9
  Opens key:
809a-482b-b60b-bcad1f8d0cd7}
  Opens key:
                                  f553-446a-9c75-9dec124ff8h73
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8cc29128-
  Opens key:
0b57-4a2b-a7b9
                    a74a70ha6fa13
  Opens key:
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6a50bbff5d15}
  Opens key
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da-
  Opens key:
b965-4fc3-8781-88dd50a6299d}
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
  Opens kev:
3f06-411b-9dd5
  Opens kev:
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
a6ca-48e0-a7c4
                     4cdd258439e2}
  Opens kev:
                                  HKLM\s\
                                             stem\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
a840-44a9-97b1
                         4fddaa8c8}
  Opens key:
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
60e9-4301-a338-beab1c70b3e9}
  Opens key
                                  HKI M\
                                                         entcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a068e}
Opens key:
11b9-4e74-b083-99f
                                  HKI M\s
                                                     currentcontrolset\control\wdi\diagnosticmodules\{c0f51d84-
                         11ba2db0a}
  Opens key
                                  HKLM\
                                                     urrentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}
Opens key:
5be9-4f25-862e
                                  HKLM\syst
                                                em\currentcontrolset\control\wdi\diagnosticmodules\{c8544339-
                     485f1b1a6935}
                                  HKLM\sy
                                                         entcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}
  Opens key:
                                  HKLM\sy
                                                         entcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}
                                  HKLM
  Opens key
                                                        rentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e
3852-4952-b76b-23bb8e35d344}
  Opens key:
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
3287-4e3f-af68-632c90f3ac95}
                                  HKLM\system\currentcontrolset\control\wdi\config
  Opens key
  Opens key
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
```

```
Opens key
                                   HKLM\system\currentcontrolset\control
  Opens key:
                                   HKLM\software\microsoft\restartmanager
  Opens key
                                   HKLM\software\microsoft\windows\windows error reporting\wm
                                   HKCU\software\microsoft\windows\currentversion\radar
  Opens key:
  Opens key
                                   HKLM\software\microsoft\radar\heapleakdetection\settings
                                   HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}
  Opens key
  Opens key:
Opens key:
                                   HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}
                                   HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ed
e212013ea917}\treatas
                                   HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\treatas
  Opens key:
Opens key: HKCI
e212013ea917}\inprocserver32
                                   HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
                                   Opens key
                                   HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee
  Opens key
e212013ea917}
                                   HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprochandler32
  Opens key:
                                   HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b
e212013ea917}\inprochandler
  Opens key:
                                   Opens key
                                   \label{local-continuous} HKCU \software \clsid \c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6 \clsid \c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6 \clsid \c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6 \clsid \c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6 \cline{Continuous}
  Opens key
  Opens key
                                   HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69
a5c5bc1c2ae6}\treatas
  Opens key:
                                   HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas
                                   HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69
  Opens key:
a5c5bc1c2ae6}\inprocser
                                 er32
                                   HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69
a5c5bc1c2ae6}\inprochandler32
                                   HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32
HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-
  Opens key:
  Opens key
a5c5bc1c2ae6}\inprochandler
                                   HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler
  Opens key:
                                   HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
  Opens key:
  Opens key
                                   HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b
4a431715d9a3}\proxvstubclsid32
                                   HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
  Opens key:
  Opens key:
                                   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}
                                   HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
  Opens key
  Opens key
                                   HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805
5e9f541bd8c9}\proxystubclsid32
  Opens key:
                                   HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}
  Opens key
  Opens key:
                                   HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}
  Opens key
                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{603d3801 - bd81 - 11d0 - a3a5\}
00c04fd706ec}\treatas
                                   HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\treatas
  Opens key:
                                   HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32
                                   HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32
  Opens key:
  Opens kev:
                                   HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5
00c04fd706ec}\inprochandler32
  Opens key:
                                   HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler32
                                   HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
  Opens key:
00c04fd706ec}\inprochandler
                                   HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler
  Opens key:
                                   Opens key:
  Opens key
  Opens key:
                                   {\it HKLM \ } system \verb|\ current control set \verb|\ enum \ | \ yrintenum \ | \ print queues
                                   HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties
  Opens key:
  Opens key:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{afd97640-86a3-4210-b67c-
289c41aabe55}\0002
  Opens kev:
289c41aabe55}\0003
67d146a850e0}\0011
  Opens kev:
ae9e1faefc6c}\0002
  Opens key:
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
  Opens key
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b3
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae
  Opens key
355b7f55341b}\treatas
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
  Opens key:
  Opens key
355b7f55341b}\inprochandler32
  Opens kev:
                                   HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
                                   HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae
  Opens key:
355b7f55341b}\inprochandler
  Opens key:
                                   Opens key
                                   HKCU\software\classes\applications\calc.exe
  Opens key:
                                   HKCR\applications\calc.exe
  Opens key
                                   HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
                                   HKLM\software\policies\microsoft\windows\control panel\desktop
  Opens key
  Opens key
                                   HKCU\software\policies\microsoft\windows\control panel\desktopHKCU\software\microsoft\internet explorer\toolbar
  Opens key
  Opens key
                                   \label{thm:hkcusoftware} $$HKCU \cdot software \cdot classes \cdot clsid \{ f5a8b627-4d46-4d65-92f3-73626ae31971 \} $$HKCR \cdot clsid \{ f5a8b627-4d46-4d65-92f3-73626ae31971 \} $$
  Opens key:
Opens key: 73626ae31971}\treatas
                                   HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5a8b627 - 4d46 - 4d65 - 92f3 - 4d66 - 4d65 - 92f3 - 4d66 - 4
                                   HKCR \c1sid \f5a8b627-4d46-4d65-92f3-73626ae31971 \treat as
  Opens key:
                                   HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-
  Opens key
73626ae31971}\inprocser
                                  er32
                                   HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprocserver32
  Opens kev:
                                   HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3
  Opens key
73626ae31971}\inprochandler32
  Opens key:
                                   Opens key
                                   HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3
73626ae31971}\inprochandler
                                   HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprochandler
  Opens key:
```

HKLM\software\microsoft\windows\currentversion\explorer\commandstore

Opens key

```
Opens key:
                                                                 HKLM\software\microsoft\windows\currentversion\explorer\commandstore\
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar
HKLM \ software \ microsoft \ windows \ current version \ explorer \ command store \ shell \ windows \ . \ status bar \ bar 
     Opens key:
\label{thklm} HKLM \software \mbox{\tt windows} \current version \shell compatibility \objects \cal{thklm} 4031-e946b44c8d5} \\
     Opens key:
                                                                 HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}
                                                                 HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}
     Opens key
Opens key:
6ccfeeaa142a}\treatas
                                                                 HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
                                                                 HKCR \verb|\clsid|{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a} \verb|\treatas| \\
     Opens key
     Opens key
                                                                 HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
 6ccfeeaa142a}
                                                                er32
                                                                 HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprocserver32
     Opens key:
      Opens key
                                                                 HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-
6ccfeeaa142a}\inprochandler32
     Opens key:
                                                                 HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\tinprochandler 32a-6ccfeeaa142a\}\tinprochandler 32a-6ccfeeaa142a
     Opens key
                                                                 HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a
6ccfeeaa142a}\inprochandler
                                                                 HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprochandler
     Opens kev:
                                                                 HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
     Opens key:
     Opens key
                                                                 HKCR\clsid\{76765h11-3f95-4af2-ac9d-ea55d8994f1a}
                                                                 HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d
     Opens key
ea55d8994f1a}\treatas
     Opens key:
                                                                 HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas
     Onens key
                                                                 HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d
ea55d8994f1a}\inprocserver32
                                                                 HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32
HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
     Opens key
     Opens key
 ea55d8994f1a}\inprochandler32
                                                                 HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32
     Opens key:
                                                                 HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
 ea55d8994f1a}\inprochandler
     Opens key:
                                                                 HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\ \ in prochandled the statement of the 
     Opens kev:
                                                                 \label{thm:local-equation} $$HKCU\software\clsid_{031e4825-7b94-4dc3-b131-e946b44c8dd5}$$HKCR\clsid_{031e4825-7b94-4dc3-b131-e946b44c8dd5}$$
     Opens key:
     Opens key
                                                                 HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
                                                                 HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
     Opens key
     Onens key
                                                                 HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\treatas
                                                                 HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\treatas
     Opens key
                                                                 HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2
     Opens key
5d7904798f4b}\inprocser
                                                              /er32
                                                                 HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprocserver32
     Opens key:
                                                                 HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2
5d7904798f4b}\inprochandler32
                                                                 HKCR \verb|\clsid|{b8967f85-58ae-4f46-9fb2-5d7904798f4b} \verb|\inprochandler32| \\
     Opens key:
                                                                 HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2
     Opens key
5d7904798f4b}\inprochandler
                                                                 HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprochandler
     Opens kev:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 1414 008d ffffffff fffffff 0^ccc77560bc3634a486857716562968286
     Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0 00 07db c6^182fdc0875f0a76803e4a9848a8c1ea7
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00
                                                                 HKLM\software\microsoft\windows\currentversion\policies\explorer
HKCU\software\microsoft\windows\currentversion\policies\explorer
     Opens key:
     Opens kev:
     Opens key:
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be3
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties
     Opens key:
                                                                 \label{local-equal-equal-equal-equal-equal-equal-equal} HKLM \ system \ current controls et \ enum \ swd \ printenum \ \{af023001-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-
b8e8-d92d736469be}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002
     Opens key:
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003
                                                                 HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
     Opens key:
11e3-be67-0800272f6e60}
                                                                 HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
     Opens key
11e3-be67-0800272f6e60}\properties
Opens key: HKLM\system\currentcontrolset\control\devicecontainers\\\ 623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\0000a
Openskey: HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\prop
                                                                rties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011
HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
     Opens key
b8e8-d92d736469be\} \\ properties \\ \{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c\} \\ \\ 0002
     Opens key
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{3b2ce006-5e61-4fde-bab8-9b8aac9b26df}\0001
     Opens key
                                                                 HKLM\svstem\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011
     Opens kev:
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}
     Opens kev
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties
Opens key:
b32c-cd2da77617c7}\prope
                                                               HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-erties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002
Opens key:
11e3-be67-0800272f6e60}
                                                                 HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
Opens~key: HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-b32c-cd2da77617c7}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003
Opens key: HKLM\syste
11e3-be67-0800272f6e60}\properties
                                                                 Opens key: HKLM\system\currentcontrolset\control\devicecontainer 11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a
                                                                 \label{localization} \begin{tabular}{ll} HKLM \label{localization} & HKLM \label{loc
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
     Opens key:
b32c-cd2da77617c7}\properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0002
                                                                 HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
     Opens key:
b32c-cd2da77617c7}\properties\{3b2ce006-5e61-4fde-bab8-9b8aac9b26df}\0001
```

HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-

Opens key

```
b32c-cd2da77617c7}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011
HKLM\software\microsoft\windows\currentversion\explorer\devicenotificationcallbacks
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\deviceupdatelocations
                                           HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
   Opens key:
   Opens key:
                                           HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
   Opens key
   Opens key:
                                           HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-
a2dd-08002b30309d}
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-
a2dd-08002b30309d}
                                           HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-
   Opens key:
08002b30309d}\shellfolder
                                           HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}\shellfolder
   Opens key:
   Opens key:
                                           HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7
79ce68d8abc2}\treatas
   Opens key:
                                           HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
   Opens kev:
                                           HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32
  Opens key:
                                           HKCR\clsid\{317d06e8-5f24-433d-hdf7-79ce68d8abc2}\inprocserver32
                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{21ec2020-
   Opens key:
3aea-1069-a2dd-08002b30309d}\shellfolder
  Opens key:
                                           HKLM\software\microsoft\windows\currentversion\explorer\clsid\{21ec2020-
3aea-1069-a2dd-08002b30309d}\shellfolder
   Opens key:
                                           HKCU\software\microsoft\windows\currentversion\policies\nonenum
                                           HKLM\software\microsoft\windows\currentversion\policies\nonenum HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
   Opens key:
   Opens key
79ce68d8abc2}\inprochandler32
                                           HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler32
   Opens key:
   Opens key:
                                           HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler
   Opens key:
                                           HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler
   Opens kev:
                                           HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
                                           HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
   Opens key:
49h9-88dd-029876e11c013
                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd\}
   Opens key:
   Opens key:
                                           HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}
HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e
   Opens key
850b2087f5dd}\treatas
                                           HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\treatas
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{35786d3c-b075-
49b9-88dd-029876e11c01}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
   Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders
  Opens kev:
HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{289af617-
1cc3-42a6-926c-e6a863f0e3ha3
   Opens key:
HKLM \label{local-solution} HKLM \label{local-solution} HKLM \label{local-solution} Label{local-solution} HKLM \label{local-solution} Solution \label{local-solution} Solution \label{local-solution} HKLM \label{local-solution} Solution \label{local-solution} Solution \label{local-solution} Solution \label{local-solution} Solution \label{local-solution} Solution \label{local-solution} HKLM \label{local-solution} Solution \label{local-solution} HKLM \label{local-solution} Solution \label{local-solution} So
b075-49b9-88dd-029876e11c01}
   Opens kev:
                                          HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e
850b2087f5dd}\inprocserver32
                                           HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32
   Opens key:
   Opens key:
00a3-46b9-bc5f-9c04daddd5d7}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\fb155bdf8-
02f0-451e-9a26-ae317cfd7779}
  Opens kev:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ my computer \ name space \ delegate folders \ delegate \ folders \ folders \ delegate \ folders \ delegate
  Opens key:
                                          HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\mycomputer\namespace
   Opens key:
HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ session in follow power \ names pace \ delegate folders
                                           HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
   Opens key:
Opens key: HKCU
850b2087f5dd}\inprochandler32
                                           HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
                                           HKCR \verb|\clsid|{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd} \verb|\inprochandler32| \\
   Opens key:
                                           HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e
   Opens key:
850b2087f5dd}\inprochandler
                                           HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler
   Opens kev:
                                           HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
   Opens key:
   Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{9c73f5e5-7ae7-
4e32-a8e8-8d23b85255bf}
   Opens key:
                                           HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8
8d23b85255bf}\shellfolder
  Opens key:
                                           HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
   Opens key
HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations
Opens\ key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
Opens key: HKLM\software\m 7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
                                          HKLM\software\microsoft\windows\currentversion\explorer\clsid\{9c73f5e5-
                                           HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32
   Opens key:
                                           HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
   Opens key:
                                           Opens key:
                                           HKCU\software\microsoft\windows\currentversion\shell extensions\cached
   Opens kev:
   Opens key:
                                           8d23b85255bf1
                                           HKCR \ activatable classes \\ \ clsid \\ \{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf\}
   Opens key:
   Opens key
                                           HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\treatas
  Opens key:
Opens key:
                                           HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\treatas
                                           HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
```

HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-

8d23b85255bf}\inprocserver32

Opens key:

```
8d23b85255bf}\inprochandler32
                                                                                                                    HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler32
        Opens key:
        Opens key
                                                                                                                    HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
  8d23b85255bf)
        Opens key:
                                                                                                                   HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler
        Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
        Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
 11e3-be65-806e6f6e6963}\
        Opens key:
                                                                                                                    HKCU\software\classes\drive\shellex\folderextensions
                                                                                                                    HKCR\drive\shellex\folderextensions
        Opens key:
                                                                                                                    HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
        Opens key
 4442-804e-409d6c4515e9}
                                                                                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 409d6c4515e9)
        Opens key:
 a8e8-8d23b85255bf}
        Opens key:
 HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace
        Opens kev:
 HKLM \label{limits} In the limits of tware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\userslibraries| names pace \verb|\delegatefolders| delegatefolders| and the limits of tware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\userslibraries| names pace \verb|\delegatefolders| delegatefolders| and the limits of tware \verb|\delegatefolders| delegatefolders| and the limits of tware \verb|\delegatefolders| delegatefolders| delega
       Opens kev:
 \label{thm:linear} \parbox{$HKCU$\software\mbox{$microsoft\windows\currentversion\explorer\userslib} are space} \parbox{$hkcu$\software\mbox{$microsoft\windows\currentversion\explorer\userslib} are space} \parbox{$hkcu$\software\mbox{$microsoft\windows\currentversion\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\exp
        Opens key:
 12e1-490f-8782-c0835afd98fc}
        Opens key:
 HKCU \label{local-soft-ware-law-soft-windows} Law \label{local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows-local-windows
        Opens key:
 \label{thm:hkcu} \begin{tabular}{ll} HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\label{thkcu} info\label{thkcu} \end{tabular} Akcula in the constraints of the
        Opens key:
 \label{thm:hkculsoftware} HkCulsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\session| info \verb|\lusers| libraries \verb|\namespace| delegate folders \verb|\currentversion| explorer \verb|\session| info \verb|\lusers| libraries \verb|\namespace| delegate folders \verb|\currentversion| explorer \verb|\session| explorer \verb|\currentversion| explorer 
        Opens key:
                                                                                                                    HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
          Opens key:
                                                                                                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
        Opens key
 HKCU\software\microsoft\windows\currentversion\explorer\hidedesktopicons\newstartpanel
        Opens key:
 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} which is a function of the constant panel of the constant p
Opens key: HKCl
3aea-1069-a2d8-08002b30309d}
                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
 3aea-1069-a2d8-08002b30309d}\
 \label{lem:condition} Opens \; key: & HKCU \software \mbox{\sc microsoft} \\ 3aea-1069-a2d8-08002b30309d \sc microsoft \sc micro
                                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
                                                                                                                    HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid 
 3aea-1069-a2d8-08002b30309d}\defaulticon
        Opens key:
 HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows \ homeometric between the contractions \ and \ homeometric between the contractions \ have a supported by the contraction \ have been contracted as the contraction \ have been contracted by th
                                                                                                                    HKLM\system\currentcontrolset\services\bits\startoverride
          Opens key:
        Opens kev:
                                                                                                                    HKLM\system\currentcontrolset\services\http
                                                                                                                    HKU\s-1-5-20
          Opens key
                                                                                                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20
        Opens key:
          Opens key:
                                                                                                                    HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\use
 shell folders
        Opens key:
                                                                                                                    HKU\s-1-5-20\environment
        Opens key
                                                                                                                    HKU\s-1-5-20\volatile environment
                                                                                                                    HKU\s-1-5-20\volatile environment\0
        Opens key:
        Opens key:
                                                                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\sppsvc.exe
        Opens key:
                                                                                                                    5-20
        Opens key
                                                                                                                    HKLM\system\currentcontrolset\control\mui\settings
        Opens key:
                                                                                                                    HKLM\software\classes
                                                                                                                    HKCR\appid\sppsvc.exe
        Opens key:
        Opens kev:
                                                                                                                    HKLM\software\microsoft\windows\currentversion\action
  center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
                                                                                                                    HKLM\software\microsoft\windowsruntime\clsid\{9dac2c1e-7c5c-40eb-833b-
        Opens kev:
 323e85a1ce84}
        Opens kev:
                                                                                                                    HKCR\activatableclasses\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
                                                                                                                    HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
          Opens key:
        Opens key:
                                                                                                                    HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
        Opens key:
                                                                                                                    HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b
 323e85a1ce843\treatas
                                                                                                                    HKCR\clsid\{9} dac2c1e-7c5c-40eb-833b-323e85a1ce84\} \treatas
        Opens key:
        Opens key
                                                                                                                    HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b
 323e85a1ce84}\inprocserver32
                                                                                                                   HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
        Opens key:
        Opens key
 323e85a1ce84}\inprochandler32
                                                                                                                    HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
        Opens key:
 Opens key: HKG
323e85a1ce84}\inprochandler
                                                                                                                    HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
                                                                                                                    HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler
        Opens key:
        Opens kev:
                                                                                                                    HKLM\software\microsoft\security center
HKLM\software\policies\microsoft\internet explorer\security
          Opens key:
        Opens kev:
                                                                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zones\0
       Opens kev:
                                                                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zones\1
        Opens key:
                                                                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zones\2
 Opens key:
settings\zones\3
                                                                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
                                                                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\0
                                                                                                                    \label{local-observation} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
                                                                                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zones\1
        Opens key:
                                                                                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zones\2
        Opens key:
                                                                                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zones\3
        Opens key:
                                                                                                                    \label{local-observation} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
 settings\zones\4
        Opens key:
                                                                                                                     HKCU\software\policies\microsoft\internet explorer
                                                                                                                    HKCU\software\microsoft\internet explorer\security
HKLM\software\microsoft\internet explorer\security
          Opens key
          Opens key
```

```
Opens key:
                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones
                                          HKLM\software\microsoft\windows\currentversion\internet settings\zones
   Opens key:
  Opens key
                                          HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}
  Opens kev:
                                          HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{ca236752 - 2e77 - 4386 - b63b - b6
0e34774a413d}
  Opens key:
Opens key:
                                          \label{local-continuity} HKCR\activatable classes \\ clsid \\ \{ca236752-2e77-4386-b63b-0e34774a413d\} \\ HKCU \\ software \\ classes \\ clsid \\ \{ca236752-2e77-4386-b63b-0e34774a413d\} \\
  Opens key
                                          HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
                                          HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b
  Opens key
0e34774a413d}\treatas
                                          HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
  Opens key:
   Opens key
                                          HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32
                                          HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
   Opens key:
  Opens key
                                          HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler32
                                          HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
  Opens key:
   Opens key:
                                          HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b
0e34774a413d}\inprochandler
  Opens key:
                                          HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
  Opens kev:
                                          HKLM\software\microsoft\wbem\cimom
                                          HKLM\software\policies\microsoft\windows\windows error reporting
  Opens key:
  Opens key
                                          HKLM\software\microsoft\windows\windows error reporting
                                          HKCU\software\policies\microsoft\windows\windows error reporting
  Opens key
                                          HKCU\software\microsoft\windows\windows error reporting
HKLM\software\microsoft\windows\windows error reporting\syspreplock
  Opens key
  Opens key
  Opens key
                                          HKCU\software\microsoft\windows\windows error reporting\erc
  Opens key:
\label{thm:hkculsoftware} \begin{tabular}{ll} HKCU\software \mbox{$\mathbb{N}$ indows \current version \explorer \session in folders} \end{tabular}
                                          HKLM\software\microsoft\windowsruntime\clsid\{88d96a05-f192-11d4-a65f-
  Opens key:
0040963251e5}
                                          HKCR\activatableclasses\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
  Opens key:
                                          HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
   Opens key
  Opens key
   Opens key:
                                          HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f
0040963251e5}\treatas
                                          Opens key:
  Opens key
                                          HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f
0040963251e5}\inprocserver32
  Opens key:
                                          HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
                                          HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f
  Opens key
0040963251e5}\inprochandler32
                                          HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:
Opens key: HK0
0040963251e5}\inprochandler
                                          HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
  Opens key:
                                          Opens key:
                                          HKLM\software\microsoft\msxm160
                                          HKLM\software\microsoft\windows\currentversion\action
   Opens key:
center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
                                          HKLM\software\microsoft\windowsruntime\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c41
                                          HKCR\activatableclasses\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
  Opens key:
  Opens key
                                          HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
                                          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
                                          HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
  Opens key
499afcec98c4}\inprocserver32
                                          HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
  Opens key:
  Opens key
                                          HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be
499afcec98c4}\inprochandler32
                                          Opens key:
                                          HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
  Opens key
499afcec98c4}\inprochandler
                                          HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
  Opens kev:
                                          HKLM\software\microsoft\windows\currentversion\policies\system
   Opens key
                                          HKLM\software\microsoft\windows\currentversion\action
  Opens key
center \providers \com{\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc\}}
  Opens kev:
                                          HKLM\software\microsoft\windowsruntime\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc)
  Opens key
                                          HKLM\software\microsoft\windowsruntime\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}
  Opens key
                                          HKCR\activatableclasses\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
                                          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-bc11
  Opens key
40cd513679d5}\treatas
                                          HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
  Opens key:
  Opens key
                                          Opens key:
                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
   Opens key
                                          HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2
  Opens key
f0aa6db5d4bc}\treatas
  Opens kev:
                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas
                                          HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprocserver32
  Opens key:
                                          HKCU \setminus software \setminus classes \setminus clsid \setminus \{900c0763-5cad-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-4a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a34-bc1f-6a3
40cd513679d5}\inprocserver32
  Opens key:
                                          HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
  Opens key
                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32
  Opens key:
                                          HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f
40cd513679d5}\inprochandler32
  Opens key:
                                          HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
  Opens key
                                          HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f
40cd513679d5}\inprochandler
                                         Opens key:
  Opens key
f0aa6db5d4bc}\inprochandler32
                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler32
  Opens kev:
                                          HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprochandler
                                          HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler
  Opens key:
   Opens kev:
                                          HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
   Opens key:
                                          HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
  Opens key
                                          HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc
00aa00404770}\proxystubclsid32
                                          HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
  Opens key:
   Opens key
                                          HKLM\software\microsoft\windowsruntime\clsid\{a4a1a128-768f-41e0-bf75-
```

```
e4fddd701cba3
                                                                         HKCR \ activatable classes \ \ \ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}
     Opens key
                                                                        \label{local-hkcu} HKCU \ software \ clsid \ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\} \ HKCR \ clsid \ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\}
     Opens key
     Opens key:
    Opens key
                                                                        \label{thm:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hklm:software:hkl
    Opens key:
Opens key:
e4fddd701cba}\treatas
                                                                        HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
    Opens key:
                                                                        HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
                                                                        HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
    Opens kev
e4fddd701cba}\inprocserver32
                                                                        HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
    Opens key:
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\com\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
Opens key:
7517526cf1c1}
                                                                        HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-43f7-9c40-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-c061-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d26de5c1-d2
    Opens key:
                                                                         Opens key
     Opens key:
    Opens key
                                                                        HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40
7517526cf1c1}\treatas
                                                                        HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas
    Opens kev:
                                                                        HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
     Opens key:
e4fddd701cba}\inprochandler32
    Opens key:
                                                                        HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKG
e4fddd701cba}\inprochandler
                                                                        HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
                                                                        HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
    Opens key:
    Opens key
7517526cf1c1}\inprocser
                                                                     /er32
                                                                        HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32
    Opens key:
      Opens key
                                                                        HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40
7517526cf1c1}\inprochandler32
    Opens key:
                                                                        Opens key
                                                                        HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprochandler
    Opens kev:
                                                                        HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler
                                                                         HKCU\software\microsoft\windows\currentversion\startupnotify
     Opens key
    Opens key
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
    Opens key
                                                                        HKI M\software\microsoft\windowsruntime\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3}
    Opens key
                                                                        \label{local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-ses-local-s
     Opens key:
     Opens key
                                                                        HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
                                                                        HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0
    Opens key
5017a56357c31
                                                                        HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
    Opens key:
Opens key:
5017a56357c3
                                                                        HKCU\software\classes\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-
    Opens key
                                                                        \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \current version \begin{tabular}{ll} action \begin{tabular}{ll} colline \begin{t
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
    Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
    Opens key:
                                                                         HKLM\software\microsoft\windows\currentver
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
    Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action
                                                    eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
center\provide
    Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}
Opens key: HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
                                                                        HKLM\software\microsoft\windows\currentversion\action
    Opens key:
center\provide
                                                       entlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
                                                                        HKLM\software\microsoft\windows\currentversion\action
    Opens key:
                                                     ventlog\{b447b4db-7780-11e0-ada3-18a90531a85a}
    HKLM\software\microsoft\windows\currentversion\action
    Opens kev:
center\providers\eventlog\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}
    Opens kev:
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}
    Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{96f4a050-7e31-453c-88be-9634f4e02139}
    Opens kev:
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
    Opens key:
Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action center
                                                                        HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
    Opens key:
                                                                        HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
Opens key:
                                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1
                                                                        \label{eq:hklm-system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10} HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11
    Opens key
    Opens key
     Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13
    Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15
     Opens key:
     Opens key
     Opens key
                                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16
    Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17
                                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18
     Opens key:
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19
     Opens key
    Opens key:
                                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2
    Opens key:
Opens key:
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21
    Opens key
                                                                        \label{eq:hklmsystem} \begin{tabular}{ll} HKLM\system\pa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22 \\ HKLM\system\pa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23 \\ \end{tabular}
    Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25
     Opens key
                                                                        \label{eq:hklm-system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26} HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\\ HKLM\system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\\ HKLM\system-wpa-8dec0af1-0341-4b93-8dec0af1-0341-4b93-
     Opens key
    Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29
    Opens key:
     Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30
     Opens key
    Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33
     Opens key:
     Opens key
     Opens key:
    Opens key
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4
     Opens key:
                                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5
                                                                        HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6
     Opens key
     Opens key
                                                                         HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7
```

```
Opens key:
                                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8
                                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9
       Opens key:
      Opens key
                                                                                                HKCU\software\microsoft\windows
                                                                                               reprotectionplatform\persistedtsrearmed
nt\currentve
                                                                                                HKCU\software\microsoft\windows
     Opens key
nt\currentversion\softwareprotectionplatform\persistedsystemstate
Opens~key: \\ HKLM\software\microsoft\windows \\ nt\currentversion\softwareprotectionplatform\plugins\modules \\
      Opens key
                                                                                                HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-12006ef9b32a
      Opens key:
                                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662
                                                                                                HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects
      Opens key:
                                                                                                HKLM\software\microsoft\windo
nt \verb|\color= | the constraint | the constraint | the color | the
      Opens key:
                                                                                                HKLM\software\microsoft\windows
\label{lem:nt_current_version} nt `current version `software protection platform `plug in s` objects `msft: rm/algorithm/bios/4.0 Opens key: <math display="block"> HKLM \setminus Software \setminus MLLM \setminus M
\label{lem:nt-current-version-software-protection-platform-plugins-objects-msft:rm/algorithm/flags/1.0 \\ Opens key: HKLM\software\microsoft\windows
Opens key: HKLM\software\microsoft\windows

HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/phone/1.0| and the protection platform objects obje
      Opens key:
                                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
Opens key: HKLM\software\microsoft\windows
nt\currentve
                                                     sion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009
                                                                                                HKLM\software\microsoft\windows
      Opens key:
nt\currentversi
                                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect
                                                                                                HKLM\software\microsoft\windows
      Opens key:
nt\currentve
                                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0
     Opens key:
                                                                                                HKLM\software\microsoft\windows
nt\currentve
                                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0
      Opens key
                                                                                                HKLM\software\microsoft\windows
nt\currentve
                                                                                               reprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0
      Opens kev:
                                                                                                HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0
     Opens kev:
                                                                                                HKLM\software\microsoft\window
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft|: spp/action/reeval/1.0| and the sum of the sum of
      Opens key
                                                                                                HKI M\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0
                                                                                                HKLM\software\microsoft\window
      Opens key
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0
      Opens key:
                                                                                                HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0
      Opens key
                                                                                                HKLM\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0
                                                                                                HKLM\software\microsoft\window
nt \verb| current version \verb| software protection platform \verb| plugins \verb| objects \verb| msft: spp/collector/kms/1.0| | to the first object of the first object object object of the first object 
                                                                                                HKLM\software\microsoft\windows
      Opens key
nt\currentyersion\softwareprotectionplatform\plugins\objects\msft;spp/licenseacquisition/payloadhandler/eul/1.0
      Opens key:
                                                                                                HKLM\software\microsoft\windows
\label{lem:ntcurrent} $$ nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0 $$ Opens key: $$ HKLM\software\microsoft\windows $$ HKLM\software\microsoft\windows $$ $$ HKLM\software\microsoft\windows $$ $$ $$ his particular to the property of the property of
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0

Opens key: HKLM\software\microsoft\windows
                                                    sion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0
nt\currentve
      Opens key:
                                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0 Opens key: HKLM\software\microsoft\windows
nt\currentve
                                                           on \ software protection platform \ plugins \ objects \ msft: spp/license acquisition/sequence/1.0
                                                                                                HKLM\software\microsoft\windows
     Opens key:
nt\currentve
                                                                                                reprotectionplatform\plugins\objects\msft:spp/statecollector/pkey
                                                                                                HKLM\software\microsoft\windows
      Opens key
nt\currentve
                                                                                             reprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
      Opens kev:
                                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwa
                                                                                               reprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0
      Opens kev:
                                                                                                HKLM\software\microsoft\window
nt \verb|`current| version \verb|| software protection platform \verb|| plugins \verb|| objects \verb|| ms/resp/volume/services/kms/activation info/1.0 | objects objects/kms/activation info/1.0 | objects/kms/activation info/1.0 | objects/kms/activation info/1.0 | objects/kms/activation info/1.0 | objects/kms/activation info/1.
     Opens kev:
                                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwa
                                                                                                reprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0
      Opens key:
                                                                                                HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
       Opens key:
                                                                                                HKLM\software\microsoft\rpc\extensions
       Opens key
                                                                                                HKCR\interface\{00000134-0000-0000-c000-00000000046}
                                                                                                HKCR\interface\{00000134-0000-0000-0000000000046}\proxystubclsid32
      Opens key
      Opens key
                                                                                                HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
                                                                                                HKLM\software\microsoft\windows nt\currentversion\
      Opens key:
       Opens key
Opens key: HKCU\software\microsoft\windows nt\currentversion\softwareprotectionplatform\reboot.sl_brt_commit
                                                                                                HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0
      Opens key:
      Opens key
Opens kev:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08
      Opens key:
                                                                                                HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0
                                                                                                 HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0
       Opens key:
      Opens key
                                                                                                HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0
      Opens key:
                                                                                                HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0
      Opens key
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1
      Opens key:
Opens key:
                                                                                                \label{local-HKLM-system-current} HKLM \ system \ current control set \ enum\ acpi \ pnp0100 \ 4\&e03a844\&0 \ HKLM \ system \ current control set \ enum\ acpi \ pnp0000 \ 4\&e03a844\&0 \ decode \ decode
      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 key:
       Opens key
                                                                                                                                                                                                                                                                                                                                   1.0.7.3_\5&34baf594&0&0.0.0
HKLM\system\currentcontrolset\enum\ide\diskhitachi
                                                                                                HKLM\svstem\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1
      Opens kev:
       Opens key
HKLM\system\currentcontrolset\enum\pci\ven 80ee&dev beef&subsys 00000000&rev 00\3&267a616a&1&10
                                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34
      Opens key:
       Opens kev:
                                                                                                HKLM\system\wpa\
                                                                                                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1\
       Opens key:
      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\
```

```
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14\
  Opens key:
                           \label{local-equation} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16\\ \label{local-equation} \end{subarray}
  Opens key
  Opens key:
 Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18\
 Opens key
 Opens key:
Opens key:
                           \label{eq:hklmsystem} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\\ \label{eq:hklmsystem}
 Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21\
 Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23\
 Opens key
 Opens key
  Opens key:
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24\
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25\
 Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\
  Opens key
 Opens key
  Opens key:
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28\
                           \label{local-equation} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3\\ \label{local-equation}
 Opens key
  Opens key:
 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:
 Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4\
 Opens key:
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5\
  Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7\
 Opens key
                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9\
 Opens key
 Opens key:
Opens key:
0040963251e5)
                           HKLM\software\microsoft\windowsruntime\clsid\{88d96a06-f192-11d4-a65f-
                           HKCR\activatableclasses\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
  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:
 Opens key
  Opens key:
                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key
                           HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler
                           HKCU\control panel\international
  Opens key
                           HKLM\software\microsoft\windowsruntime\clsid\{88d96a08-f192-11d4-a65f-
 Opens key
0040963251e5}
 Opens kev:
                           HKCR\activatableclasses\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
  Opens key:
 Opens key
                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\treatas
                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32
 Opens key
  Opens key
                           HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler32
HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler
 Opens key
                           HKLM\system\currentcontrolset\control\cryptography\providers
  Opens key:
  Opens key:
                           HKLM\system\currentcontrolset\control\cryptography\configuration
Opens key:
73e6154572dd)
                           HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-
                           HKCR \ activatable classes \ \ clsid \ \{0f87369f-a4e5-4cfc-bd3e-73e6154572dd\}
 Opens key:
                           HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
  Opens kev:
                           HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32
  Opens key
 Opens key
  Opens key:
                           HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32
 Opens key
                           HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler
                           HKLM\system\currentcontrolset\control\productoptions
 Opens key:
 Queries value
                           HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
                           HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
 Oueries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value
                           HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value
HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value:
  Queries value
                           HKLM\system\currentcontrolset\control\mui\uilanguages\er
us[alternatecodepage]
 Queries value:
                           {\tt HKCU \backslash control\ panel \backslash desktop[preferreduil anguages]}
 Oueries value:
                           HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
                           HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value:
 Oueries value:
                           HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
                           HKLM\software\microsoft\windows nt\currentversion\image file execution
 Oueries value
options\dllnxoptions[usefilter]
                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[1be5bc13fd1cf615a95feec0c5b7fd13.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windowsnt\currentversion\windows[loadappinit_dlls]
                           HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Queries value:
  Oueries value:
                           HKLM\svstem\currentcontrolset\control\lsa[fipsalgorithmpolicv]
                           HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value
 Oueries value:
                           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                           HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Oueries value
                           HKLM \verb|\system| current controlset \verb|\control| session manager[safedllsear chmode]|
                           HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
 Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[next catalog entry id]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ \ 0000000000001 \ [packed catalogitem]
 Queries value:
HKLM \ system \ current control set \ services \ \ win sock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ \ 0000000000003 \ [packed catalog item]
 Queries value
```

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13\

Opens key

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004[packedcatalogitem]
HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ \ protocol\_catalog9 \ \ catalog\_entries \ \ 0000000000005 \ [packed catalog item]
   Oueries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000006 \ [packed catalog item]
   Oueries value:
Queries value
Queries value
Queries value
HKL\\ M\system\current controls et\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packed catalogitem]
  Queries value:
Queries value:
\label{local-parameters} HK \dot{L} M \ system \ current control set \ services \ winsock \ 2 \ parameters \ names pace\_catalog \ 5 \ [num\_catalog\_entries]
   Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
   Oueries value
Oueries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[supportednamespace]
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[enabled]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[version]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000001[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000001[providerinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[providerid]
   Queries value:
Queries value:
HKLM \system \verb|\currentcontrolset\services\winsock2\parameters \verb|\namespace_catalog5\catalog_entries|\symbol{1} 0000000000002[supported namespace]|
   Queries value
\label{thm:hklm:system:current:hklk} Hkl. \\ \texttt{Mkl.m} 
   Queries value:
Queries value
HKLM \label{lem:hklm} System \color of the large system \color of the lar
   Oueries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003[librarypath]
   Oueries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003\addressfamily\rightarrows
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[enabled]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003fyersion1
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003\providerinfol
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[displaystring]
   Queries value:
Oueries value:
Oueries value
Oueries value:
Oueries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004[storesserviceclassinfo]
  Oueries value
Oueries value
HKL\\ M \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog \ services \ winsock 2 \ parameters \ names pace\_catalog \ services \ winsock 2 \ parameters \ names pace\_catalog \ services \ winsock 2 \ parameters \ names pace\_catalog \ services \ winsock 2 \ parameters \ names \ paced \ names \ names \ paced \ names \ names \ names \ paced \ names \ name
  Oueries value
HKL\\ M\system\current control set\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\space\namespace\_catalog5\catalog\_entries\space\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace\namespace
Queries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000005[enabled]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005[version]
Queries value:
HKLM \ system \ \ current controls et \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog 5 \ \ catalog\_entries \ \ \ 000000000005 \ [providerinfo]
   Queries value:
Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006fdisplaystring1
Oueries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ (catalog\_entries \ 000000000006 \ [address family]
HKL \verb|M/system/currentcontrolset/services/winsock2| parameters/namespace\_catalog5/catalog\_entries/00000000006[supportednamespace]|
     Queries value
Queries value
Queries value
HKL\\ M (system \current control set \services \winsock 2 \parameters \nowed a long-entries \nowed by the long-entries \nowed \nowed
     Queries value
Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
     Queries value:
                                                                           HKLM\software\microsoft\windows
nt\currentversion\windows[displayversion]
     Oueries value:
                                                                           HKCU\control panel\desktop[paintdesktopversion]
                                                                           HKLM\system\currentcontrolset\services\winsock\parameters[transports]
      Queries value:
     Oueries value:
                                                                           HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
                                                                           HKLM\system\currentcontrolset\services\winsock\setup
     Queries value:
migration\providers\tcpip[winsock 2.0 provider id]
     Queries value:
Oueries value
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} a winsock [max sock addrlength] $$ \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ \end{tabular} $$$ \end{ta
     Queries value
\label{local_ham} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] \end{tabular}
     Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ base \ cryptographic \ defaults \ provider \ microsoft \ base \ cryptographic \ defaults \ provider \ microsoft \ base \ cryptographic \ defaults \ provider \ microsoft \ base \ cryptographic \ defaults \ provider \ microsoft \ base \ defaults \ provider \ microsoft \ provi
provider v1.0[type]
     Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ base \ cryptographic \ microsoft \ mi
provider v1.0[image path]
     Oueries value:
                                                                           .
HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
\label{local-problem} HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds] \\ Queries\value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] \\
     Queries value:
      Oueries value:
                                                                           HKLM \verb|\software\microsoft\cryptography[machineguid]|
                                                                           HKLM\software\microsoft\rpc[maxrpcsize]
      Queries value:
     Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
     Queries value:
                                                                           {\tt HKLM \ } \dot{system \ } \dot{setup [oobein progress]}
                                                                           HKLM\system\setup[systemsetupinprogress]
      Queries value:
      Oueries value:
                                                                           HKLM\software\microsoft\rpc[idletimerwindow]
     Queries value:
                                                                           HKLM \verb|\system| current control \verb|\sqmservicelist[sqmservicelist]|
       Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[current protocol catalog]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\00000000010[packedcatalogitem]
Queries value:
Queries value
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries 64 \nooned \cite{Minimal catalog} \end{subarray} \ entries 64 \nooned \cite{Minimal catalog} \ entries 64 \nooned \cite{Minimal catalog} \end{subarray} \ entries 64 \nooned \cite{Minimal catalog} \ entries 64 \nooned \ entries 64 \nooned \cite{Minimal catalog} \ entries 64 \nooned \ entries 64 \no
     Queries value
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries 64 \no 00000000005 \[packed catalog item] \end{subarray}
     Queries value
HKL\\ M\system\current control set\services\winsock 2\parameters\protocol\_catalog9\catalog\_entries 64\000000000004[packed catalogitem]
     Queries value
HKL\\ M\system\current control set\services\winsock2\parameters\protocol\_catalog9\catalog\_entries64\colono000000003[packed catalogitem]
     Oueries value
Oueries value
Oueries value
\label{lem:hklm} \verb+KkLM\system\currentcontrolset\services\winsock2\parameters[current\_namespace\_catalog]
     Oueries value
HKL\\ M\xspace\_catalog5 \catalog\_entries 64 \
     Oueries value
HKL\\ Mk_system\\ current control set\\ services\\ winsock 2\\ parameters\\ namespace\_catalog 5\\ catalog\_entries 64\\ 000000000002[providerid]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\000000000001[providerid7
                                                                           HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
     Queries value:
cryptographic provider v1.0[type]
     Queries value:
                                                                           HKLM \label{localization} HKLM \label{localization} HKLM \label{localization} Software \label{localization} which is a second constant and the secon
cryptographic provider v1.0[image path]
  Queries value: HKLM\software\m
                                                                           HKLM\software\microsoft\windows
Queries value:

Tt\currentversion\profilelist[programdata]

Queries value:

HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
     Oueries value:
                                                                           HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
                                                                           HKLM\software\microsoft\windows\currentversion[programfilesdir]
      Queries value:
      Oueries value:
                                                                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
      Queries value:
                                                                           HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] HKLM\software\microsoft\windows\currentversion[programw6432dir]
     Queries value:
      Queries value:
     Queries value:
                                                                           HKLM \setminus software \setminus microsoft \setminus windows \setminus current version [commonw6432 dir] \\
                                                                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
     Queries value:
 18[profileimagepath]
                                                                           HKU\.default\software\microsoft\windows\currentversion\explorer\user
     Oueries value
shell folders[appdata]
                                                                           HKU\.default\software\microsoft\windows\currentversion\explorer\user
     Oueries value
shell folders[local appdata]
     Oueries value
                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[usefilter]
     Oueries value
                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[debugger]
                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
     Oueries value
options\rundll32.exe[uselargepages]
```

```
Oueries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[nodeoptions]
  Oueries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[disablewakecharge]
  Queries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[mitigationoptions]
  Oueries value
\label{thm:local_microsoft} $$HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternal manifest] $$
  Oueries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[disableheaplookaside]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rundll32.exe[frontendheapdebugoptions]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[shutdownflags]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[unloadeventtracedepth]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[tracingflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[minimumstackcommitinbytes]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
Ourries value: HKLM\software\microsoft\windows ....

Ourries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

intigeroptaytsalive]
options\rundll32.exe[keepactivationcontextsalive]
  Queries value: HKLM\software\microsoft\v

                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundl132.exe[maxdeadactivationcontexts]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundll32.exe[globalflag]
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundll32.exe[cwdillegalindllsearch]
  Queries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[debugprocessheaponly]
  Oueries value
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundl132.exe[searchpathmode]
  Oueries value
                                    HKU\.default\control panel\desktop[preferreduilanguages]
                                    HKU\.default\control
   Queries value
panel\desktop\muicached[machinepreferreduilanguages]
                                    HKLM\software\microsoft\windows
  Queries value
nt\currentversion\compatibility32[rundll32]
                                    HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:
  Oueries value
                                    {\tt HKLM \backslash software \backslash microsoft \backslash windows}
nt\currentversion\windows[loadappinit_dlls]
  Queries value:
                                    HKLM\system\currentcontrolset\services\bfe[imagepath]
                                    HKLM\system\currentcontrolset\services\bfe[type]
   Queries value:
   Oueries value
                                    HKLM\system\currentcontrolset\services\bfe[start]
  Queries value:
                                    HKLM\system\currentcontrolset\services\bfe[errorcontrol]
                                    HKLM\system\currentcontrolset\services\bfe[tag]
   Queries value
  Queries value:
                                    HKLM\system\currentcontrolset\services\bfe[dependonservice]
                                    HKLM\system\currentcontrolset\services\bfe[dependongroup]
   Queries value
   Oueries value:
                                    HKLM\svstem\currentcontrolset\services\bfe[group]
                                    HKLM\system\currentcontrolset\services\bfe[objectname]
   Queries value
  Oueries value:
                                    HKLM\system\currentcontrolset\services\aelookupsyc\triggerinfo\0[action]
   Queries value
                                    HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
   Oueries value
                                    HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
   Queries value
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
  Queries value
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[action]
  Queries value
\label{thm:local} \begin{tabular}{ll} HKLM \end{tabular} which is a property of the control of
  Queries value
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[guid]
  Queries value
HKL\dot{M} \land system \land current controls et \land services \land all user in stall agent \land trigger in fo \land 0 \texttt{[} data type 0 \texttt{]}
  Oueries value
Oueries value
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[datatype1]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
                                    HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
   Queries value:
  Oueries value:
                                    Queries value:
                                    HKLM \setminus system \setminus current control set \setminus services \setminus appids \lor c \setminus trigger info \setminus 0 \ [data type 0]
   Oueries value:
                                    \label{thm:local-problem} HKLM \system \current controls et\services \bdesvc\trigger info\0 [action] \\ HKLM \system \current controls et\services \bdesvc\trigger info\0 [type] \\
   Queries value:
   Oueries value:
                                    HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
   Queries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action] HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
   Queries value
   Queries value
                                    \label{thm:local_ham} HKLM \system \current controlset \services \browser \trigger in fo \0 [guid] \\ HKLM \system \current controlset \services \browser \trigger in fo \0 [data type 0] \\
   Queries value:
   Queries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
   Queries value
   Oueries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1]
   Queries value
   Oueries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]
   Queries value
  Oueries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
   Queries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]
   Oueries value
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]
   Queries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
  Oueries value
                                    Queries value:
                                    HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
  Queries value:
Queries value:
                                    \label{thm:local_ham} HKLM \system \current control set \services \browser \trigger in foliatatype 1] \\ HKLM \system \current control set \services \browser \trigger in foliatat 1] \\
                                    HKLM \system \current controlset \services \browser \trigger info\1[datatype2] \label{eq:hklm} HKLM \system \current controlset \services \browser \trigger info\1[data2] \label{eq:hklm}
  Queries value:
   Queries value:
                                    HKLM \system \current control set \services \browser \trigger in fold [data type 3] \\ HKLM \system \current control set \services \browser [image path]
   Queries value
   Queries value:
                                    HKLM\system\currentcontrolset\services\browser[type]
   Queries value
                                    HKLM\svstem\currentcontrolset\services\browser[start]
   Oueries value:
   Queries value
                                    HKLM\system\currentcontrolset\services\browser[errorcontrol]
  Oueries value:
                                    HKLM\system\currentcontrolset\services\browser[tag]
                                    HKLM\system\currentcontrolset\services\browser[dependonservice]
   Queries value
                                    HKLM\system\currentcontrolset\services\browser[dependongroup]
   Oueries value:
                                    HKLM\system\currentcontrolset\services\browser[group]
   Queries value:
   Oueries value:
                                    HKLM\system\currentcontrolset\services\browser[objectname]
                                    HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
   Queries value:
   Oueries value
                                    HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
   Queries value
                                    HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
```

```
Queries value:
                                                            HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
    Queries value
                                                            HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[action]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[type]
    Queries value:
                                                            HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[guid]
    Queries value:
HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[datatype0]
    Queries value:
Queries value:
                                                            HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[data0]
HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[datatype1]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
    Oueries value:
                                                            HKLM\software\microsoft\sqmclient\windows[studyid]
    Queries value:
                                                            HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
    Oueries value
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[data0]
    Queries value
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype1]
    Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[action]
    Oueries value
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ is some interest of the local property of th
    Queries value
\label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} which is a property of the latest and the latest approximation of the latest approxi
    Queries value
\label{local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ excises \end{ta
    Queries value
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[data0]
    Oueries value
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[datatype1]
    Oueries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[action]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[type]
    Queries value
                                                            HKLM \setminus system \setminus current control set \setminus services \setminus device install \setminus trigger info \setminus 0 [guid]
    Oueries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype0]
    Oueries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[data0]
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype1]
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[action]
                                                            HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[type]
    Queries value:
                                                            HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[guid]
    Queries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype0]
    Queries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[data0]
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype1]
    Queries value:
                                                            Oueries value:
                                                            HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
                                                            HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
    Queries value:
                                                            Oueries value:
    Queries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\services\dnscache[imagepath]
    Queries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\services\dnscache[type]
    Queries value:
                                                            HKLM\system\currentcontrolset\services\dnscache[start]
                                                            HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
HKLM\system\currentcontrolset\services\dnscache[tag]
    Queries value
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\dnscache[dependonservice]
    Queries value
    Oueries value:
                                                            HKLM\svstem\currentcontrolset\services\dnscache[dependongroup]
                                                            HKLM\system\currentcontrolset\services\dnscache[group]
    Queries value
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\dnscachefobjectname
                                                            HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[action]
    Queries value:
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[type]
    Queries value:
                                                            HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[guid]
    Oueries value:
                                                            HKLM \system \current control set \services \dsmsvc\triggerinfo\0[datatype0] \\ HKLM \system \current control set \services \dsmsvc\triggerinfo\0[data0] \\
    Queries value:
                                                            HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype1] HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data1]
    Oueries value:
    Queries value:
                                                            HKLM \system \current control set \services \dsm svc \trigger in fo \0 [datatype2] \\ HKLM \system \current control set \services \dsm svc \trigger in fo \0 [data2] \\
    Queries value
    Queries value
                                                            HKLM \system \current control set \services \dsmsvc\triggerinfo\log(datatype3) \\ HKLM \system \current control set \services \efs \triggerinfo\log(action) \\
    Queries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type] HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
    Queries value
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
    Queries value
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\fhsyc\triggerinfo\0[action]
                                                            HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[type]
    Queries value
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[guid]
                                                            HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[datatype0]
    Queries value:
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[action]
    Queries value:
                                                            HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[type]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[datatype0]
    Queries value:
    Queries value:
Queries value:
                                                            HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[type]
                                                            HKLM \system \current control set \services \gpsvc \trigger info \cite{thmosphill} if the limit \graph \cite{thmosphill} if the limit \graph \graph
    Queries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[data0] HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype1]
    Queries value
    Queries value:
                                                            Queries value:
                                                            HKLM\svstem\currentcontrolset\services\hidserv\triggerinfo\0ſtvpel
    Oueries value:
    Queries value
                                                            HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
                                                            HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
    Queries value
    Oueries value:
                                                            HKLM \setminus system \setminus current control set \setminus services \setminus hidserv \setminus trigger info \setminus 0 [data type 1]
    Queries value
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[action]
    Queries value
```

HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[type]

Queries value

```
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[datatype0]
\label{local-problem} HKLM \system \current controls et \services \homegroup provider \trigger in fo \0 [data type 1] \\ Queries value: HKLM \system \current controls et \services \trigger in fo \0 [action] \\
  Queries value:
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
  Queries value:
                                     HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
  Queries value:
  Queries value:
  Queries value:
                                     HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
                                     HKLM\system\currentcontrolset\services\ikeext[imagepath]
  Queries value:
                                     HKLM\system\currentcontrolset\services\ikeext[type]
   Queries value
  Queries value:
                                     HKLM\system\currentcontrolset\services\ikeext[start]
  Queries value
                                     HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ikeext[tag]
                                     HKLM\system\currentcontrolset\services\ikeext[dependonservice]
  Queries value
  Queries value:
                                     HKLM\system\currentcontrolset\services\ikeext[dependongroup]
HKLM\system\currentcontrolset\services\ikeext[group]
  Queries value
  Oueries value:
                                     HKLM\svstem\currentcontrolset\services\ikeext[objectname]
                                     HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[action]
  Queries value:
                                     Oueries value:
  Queries value:
                                     \label{thm:hklmsystem} HKLM \system \current controlset \services \key is o'trigger info \0 [datatype0] \\ HKLM \system \current controlset \services \key is o'trigger info \0 [data0] \\
  Oueries value
  Queries value:
                                     \label{thm:local-problem} HKLM\system\currentcontrolset\services\kepiso\triggerinfo\0[datatype1]\\ HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
  Oueries value:
  Queries value:
  Oueries value
                                     HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
  Queries value:
                                     HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
                                     HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
   Queries value
  Queries value:
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
  Queries value
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
  Queries value:
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
  Queries value
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
  Queries value
  Oueries value:
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
  Queries value:
  Oueries value
                                     HKLM \ system \ current control set \ services \ lmhosts \ trigger in fo \ \ 2[action]
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[type]
  Queries value:
                                     HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[guid]
HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[datatype0]
  Oueries value
  Queries value:
  Queries value
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[action] HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[type]
  Queries value:
  Oueries value
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[guid]
  Queries value:
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[datatype0]
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[action]
   Queries value
  Queries value:
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[type]
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[guid]
  Queries value
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[datatype0]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[action]
  Queries value
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[type]
  Queries value
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[guid]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[datatype0]
  Queries value:
\label{local-problem} HKLM \system \current controls et\services \ncdautos etup \trigger info\0[action] \\ Queries value: HKLM \system \current controls et\services \ncdautos etup \trigger info\0[type] \\
                                     HKLM \backslash system \backslash current control set \backslash services \backslash ncdautoset up \backslash trigger in fo \backslash 0 [guid]
  Oueries value:
  Queries value
\label{local-problem} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ LM \end{tabular} $$
                                     HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[data0]
  Queries value:
  Oueries value
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype1]
                                     HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
  Queries value:
  Oueries value:
  Queries value
                                     HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
  Oueries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
  Queries value
\label{local-objective} HKLM \system \current controls et\services \policy agent \trigger in fo \0 \[data type 1] \\ Queries \value: HKLM \system \current controls et\services \policy agent \[image path] \\
  Oueries value:
                                     HKLM\system\currentcontrolset\services\policyagent[type] HKLM\system\currentcontrolset\services\policyagent[start]
  Queries value:
                                     HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
HKLM\system\currentcontrolset\services\policyagent[tag]
  Oueries value:
  Queries value:
  Queries value:
                                     HKLM\system\currentcontrolset\services\policyagent[dependonservice]
  Queries value
HHKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependongroup]
  Queries value:
                                     {\tt HKLM \ } system \verb| current control set \verb| services \verb| policy agent[group]|
                                     HKLM\system\currentcontrolset\services\policvagent[objectname]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\shell
  Queries value
folders[cache]
HKLM\system\currentcontrolset\services\remoteregistrv\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[guid]
  Queries value
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[data0]
  Oueries value
HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[action]
  Queries value:
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[type] HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[guid]
  Queries value:
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[datatype0]
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[action]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[type]
  Queries value:
  Oueries value:
                                     HKLM\svstem\currentcontrolset\services\scardsvr\triggerinfo\1[guid]
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[datatype0]
  Queries value:
  Oueries value:
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[data0]
                                     HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[datatype1]
  Queries value:
```

HKLM\software\microsoft\windows

Queries value

nt\currentversion\compatibility32[conhost]

```
Queries value
                                                       HKLM\software\microsoft\ole[pagea]locatorusesystemheap]
                                                       HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
    Queries value
    Oueries value:
                                                       {\tt HKLM \backslash software \backslash microsoft \backslash ole[aggressive mtatesting]}
                                                       HKCU\console[screencolors]
    Queries value:
                                                       HKCU\console[popupcolors]
HKCU\console[insertmode]
   Queries value:
    Queries value:
                                                       \label{thm:local_hammon} HKCU \console[quickedit] \\ HKLM \console[quicked
    Queries value:
    Queries value:
   Queries value
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type] HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
    Queries value:
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[action]
    Oueries value
    Queries value:
    Queries value
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[type]
                                                       HKCU\console[codepage]
   Queries value:
    Queries value
                                                       HKCU\console[screenbuffersize]
   Queries value:
                                                       HKCU\console[windowsize]
    Queries value
                                                       HKCU\console[windowposition]
   Queries value:
                                                       HKCU\console[fontsize]
                                                       HKCU\console[fontfamily]
    Queries value
   Queries value:
                                                       HKCU\console[fontweight]
                                                       HKCU\console[facename]
    Queries value
    Oueries value:
                                                       HKCU\console[cursorsize]
    Queries value:
                                                       HKCU\console[historybuffersize]
   Oueries value:
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[guid]
    Queries value:
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[datatype0]
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[action] HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[type]
    Oueries value
    Queries value:
                                                       HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[guid] HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[datatype0]
    Oueries value:
   Queries value:
    Oueries value
                                                       HKCU\console[numberofhistorybuffers]
   Queries value:
                                                       HKCU\console[historynodup]
                                                       HKCU\console[colortable00]
    Queries value
                                                       HKCU\console[colortable01]
   Queries value:
    Queries value
                                                       HKCU\console[colortable02]
   Queries value:
                                                       HKCU\console[colortable031
    Queries value
                                                       HKCU\console[colortable04]
    Oueries value:
                                                       HKCU\console[colortable05]
                                                       HKCU\console[colortable06]
    Queries value
   Oueries value:
                                                       HKCU\console[colortable07]
    Queries value:
                                                       HKCU\console[colortable08]
    Oueries value
                                                       HKCU\console[colortable09]
    Queries value:
                                                       HKCU\console[colortable10]
   Oueries value:
                                                       {\tt HKCU \backslash console[colortable 11]}
                                                       HKCU\console[colortable12]
    Queries value:
    Queries value:
                                                       HKCU\console[colortable13]
HKCU\console[colortable14]
   Queries value:
    Oueries value
                                                       HKCU\console[colortable15]
   Queries value:
                                                       HKCU\console[loadconime]
    Queries value
                                                       HKCU\console[extendededitkey]
   Queries value:
                                                       HKCU\console[extendededitkeycustom]
                                                       HKCU\console[worddelimiters]
    Queries value
   Oueries value:
                                                       HKCU\console[trimleadingzeros]
                                                       HKCU\console[enablecolorselection]
    Queries value
   Oueries value
                                                       HKCU\console[scrollscale]
   Queries value:
                                                       HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:
                                                       Oueries value:
                                                       HKLM \verb|\system| current controlset \verb|\services| sppsvc \verb|\triggerinfo| 0[type] | type | typ
                                                       HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[guid]
    Queries value:
                                                       HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Oueries value
    Queries value:
    Oueries value:
                                                       HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
   Queries value:
    Oueries value
                                                       HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
                                                       HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
   Queries value:
                                                       HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
    Queries value
    Oueries value:
    Queries value:
                                                       HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[action]
   Oueries value:
                                                       HKLM\svstem\currentcontrolset\services\svsvc\triggerinfo\0[tvpe]
                                                       HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[guid]
    Queries value
   Oueries value:
                                                       HKLM\svstem\currentcontrolset\services\svsvc\triggerinfo\0[datatvpe0]
                                                       HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[data0]
    Queries value
   Oueries value
                                                       HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype1]
   Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[action]
   Queries value
Queries value
\label{local_ham} \begin{tabular}{ll} HKLM \end{tabular} which is a property of the local property of the lo
   Queries value
HKLM \verb|\system| current controlset \verb|\services| system events broker \verb|\triggerinfo| 0 [data type 0]| \\
Oueries value
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[action]
   Oueries value
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[guid]
   Oueries value
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[datatype0]
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[data0]
   Queries value
Queries value
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
   Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
   Queries value
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
   Queries value
```

```
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
   Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ exclusion to like the control of the c
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[action]
   Queries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[type]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[guid]
    Queries value
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[datatype0]
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[data0]
   Queries value:
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[datatype1]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[action]
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[type]
    Queries value:
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[guid]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus time broker \setminus trigger in fo \setminus 1 [data type 0]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[data0]
    Oueries value
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[datatype1]
   Queries value:
HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[action]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[type]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[action]
HKLM\svstem\currentcontrolset\services\vmickvpexchange\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[guid]
   Queries value:
\label{local-problem} HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\cuprolled [atatype0] \\ Queries\value: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\cuprolled [atatype0] \\
   Oueries value:
                                                    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[guid]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[datatype0]
   Queries value:
\label{local_hammon_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[action] \end{tabular}
                                                    HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[type]
   Queries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[guid]
   Queries value
HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[datatype0]
   Oueries value:
HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[action]
                                                    HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[type]
   Oueries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[guid]
   Oueries value
HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[datatype0]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[action]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[type]
                                                    HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[datatype0]
    Oueries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action] HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
   Queries value:
   Queries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
   Queries value:
                                                    HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
    Queries value:
    Oueries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
                                                     HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[action]
    Queries value
   Oueries value:
                                                    HKLM\svstem\currentcontrolset\services\wcmsvc\triggerinfo\0[tvpe]
                                                     HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[guid]
    Queries value:
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[datatype0]
    Queries value:
                                                     HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[data0]
    Oueries value:
                                                    HKLM \system \current control set \services \wcmsvc \trigger info \cite{thmosphill} in the limit of the lim
    Queries value:
   Oueries value:
                                                    HKLM \verb|\system| current controlset \verb|\services| we be client \verb|\triggerinfo| 0[type]|
    Queries value:
                                                    HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
    Oueries value
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
   Queries value:
                                                    \label{thm:hklm} HKLM \system \current controls et\services \wersvc\trigger info\0 [action] \\ HKLM \system \current controls et\services \wersvc\trigger info\0 [type] \\
    Queries value:
    Queries value:
                                                    HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[action]
    Queries value:
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[type]
    Queries value
                                                     HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[guid]
   Oueries value:
HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[datatype0]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[action]
    Queries value:
                                                     HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[type]
   Oueries value:
                                                    HKLM \verb|\system| current controlset \verb|\services| whids \verb|\system| followed by the controlset by the control
                                                    HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[datatype0]
    Queries value:
   Queries value:
Queries value:
                                                    HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[data0] HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[datatype1]
                                                    Queries value:
    Queries value:
                                                    Queries value:
   Queries value:
                                                    HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[data0]
HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[datatype1]
    Queries value:
    Oueries value:
    Queries value
                                                     HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
   Oueries value:
                                                    HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
                                                     HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
    Queries value:
   Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
                                                    Oueries value:
    Queries value:
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
    Queries value
```

```
HKLM\system\currentcontrolset\services\wodbusenum\triggerinfo\1[datatype0]
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
   Oueries value
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
   Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
                                  \label{thm:hklm} HKLM \system \current control set \services \swpdbusenum \trigger in fo \3 [action] \\ HKLM \system \current control set \services \swpdbusenum \trigger in fo \3 [type] \\
  Queries value
   Queries value
   Oueries value
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
   Queries value
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[action]
  Queries value
   Queries value
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[type]
                                  HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[guid]
   Queries value:
   Queries value
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype0]
   Queries value:
                                   HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[data0]
   Oueries value
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype1]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[action] HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[type]
   Queries value
   Oueries value:
                                  HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[guid]
   Queries value:
\label{local-problem} HKLM\system\currentcontrolset\services\wsservice\triggerinfo\cite{Control} Queries\ value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\cite{Control} action]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[type] HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[guid]
   Oueries value
   Queries value:
   Oueries value:
                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[datatype0]
   Queries value:
                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[action]
   Oueries value
                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[type]
                                  HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[guid]
   Queries value:
                                   Queries value
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
   Queries value:
   Queries value
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
  Queries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
   Queries value
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
   Oueries value:
                                  HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
                                   HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
   Queries value
  Oueries value:
                                  HKLM\system\currentcontrolset\services\wdisystemhost[objectname]
   Queries value:
                                   HKLM\system\currentcontrolset\services\wdisystemhost[imagepath]
   Oueries value
                                  HKLM \verb|\system| current controlset \verb|\services| wdisystem host[wow64]|
                                   HKLM\system\currentcontrolset\services\wdisystemhost[requiredprivileges]
   Queries value:
  Oueries value
                                  HKLM \  \  \, icrosoft \  \  \, int \  \  \, icrosoft \  \  \, int \  \  \  \  \, int \  \  \  \  \, int \  \  \  \, int \  \  \  \, int \  \  \,
1923240461-1905901954-2556564120-1001[profileimagepath]
                                HKU\s-1-5-21-1923240461-1905901954-2556564120-
\windows\currentversion\explorer\user shell folders[appdata]
  Queries value
1001\software\microsoft
   Queries value
                                  HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
   Queries value
                                   HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value
                                  HKLM\software\microsoft\windows
nt\currentversion\compatibility32[taskhost]
                                  HKLM\software\microsoft\com3[com+enabled]
  Oueries value
                                   HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}[]
   Queries value
  Oueries value
                                  HKCR\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\inprocse
                                  er32[inprocserver32]
  Oueries value
                                  HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprocserver32[]
                                  HKCR\clsid\{900be39d-6be8-461a-bc4d-
   Queries value
b0fa71f5ecb1}\in
                                  er32[threadingmodel]
                                  HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value
  Oueries value
                                  a37a-4f91-bdba-fbb98fe80
                                  4bf}[imagepath]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
  Queries value
a37a-4f91-bdba-fbb98fe804bf}[neverlowerpagepriority]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
a37a-4f91-bdba-fbb98fe804bf}[nameresource]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}[imagepath]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
  Queries value
6c46-4d66-b413-70b0445df33c)[neverlowerpagepriority]
Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}[nameresource]
  Queries value:
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8-e3670ed91517}[imagepath]
  Queries value:
                                  beea-4c9d-91e8-e3670ed91517}[neverlowerpagepriority]

Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8-e3670ed91517}[nameresource]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
  Queries value
393e-41c3-9885-29ec5a701926}[imagepath]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
  Queries value
                          393e-41c3-9885-29
  Queries value:
393e-41c3-9885-29
                                 1926}[nameresource]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
  Oueries value
10bc-4f96-9b21
                    -4b6b83dbf476}[imagepath]
  Oueries value
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
10bc-4f96-9b21-4b6b83db1
                                 476}[neverlowerpagepriority]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
  Oueries value
10bc-4f96-9b21-4b6b83dbf476}[nameresource]
  Oueries value
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
fd02-4b82-a0a5-783266e430ab}[imagepath]
  Oueries value
                                  fd02-4b82-a0a5-783266e430ab}[neverlowerpagepriority]
  Oueries value
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
0ab}[nameresource]
fd02-4b82-a0a5
  Oueries value
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
5780-49de-9eb5-8d53a51fd146}[imagepath]
Queries\ value: HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb5780-49de-9eb5-8d53a51fd146\}} [neverlowerpagepriority]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
  Queries value
5780-49de-9eb5-8d53a51fd146}[nameresource]
  Queries value
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46}[imagepath]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46)[neverlowerpagepriority]
Queries value: HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46}[nameresource]
Queries value: HKLM\system\cu
398d-4edb-af71-3b830219abf7}[imagepath]
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
  Queries value:
                                  HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
```

```
398d-4edb-af71-3b830219abf7}[neverlowerpagepriority]
                                         HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
398d-4edb-af71-3b830219abf7}[nameresource]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{63e0d0f7-
   Queries value
ac2f-493b-a7f2-2f3ccdb66fca}[imagepath]
                                        Oueries value
ac2f-493b-a7f2-2f3ccdb66fca}[neverlowerpagepriority]
Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\\63e0d0f7-
ac2f-493b-a7f2-2
                            3ccdb66fca}[nameresource]
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
6c5b-43bb-860b-d4
                               ae85242b1}[imagepath]
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
                                e85242b1}[neverlowerpagepriority]
6c5b-43bb-860b-d
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
6c5b-43bb-860b-d
                                        2b1}[nameresource]
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b
                                        a2e}[imagepath]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
                                        a2e}[neverlowerpagepriority]
6a91-46e6-885b
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b-d4
                                        a2e}[nameresource]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{7a54f16f-
a73a-4258-ba46
                                        a74}[imagepath]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{7a54f16f-
a73a-4258-ba46-a1e998a6a
                                       a74}[neverlowerpagepriority]
                                        Oueries value
a73a-4258-ba46-a1e998a6aa74}[nameresource]
   Oueries value
                                        809a-482b-b60b-bcad1f8d0cd7}[imagepath]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9-
809a-482b-b60b-bcad1f8d0cd7}[neverlowerpagepriority]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9-
809a-482b-b60b-bcad1f8d0cd7}[nameresource]
                                         HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}[imagepath]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}[neverlowerpagepriority]

Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}[nameresource]
                                        Queries value
0b57-4a2b-a7b9-a74a70ba6fa1}[imagepath]
Queries value: HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8cc29128-
0b57-4a2b-a7b9-a74a70ba6fa1}[neverlowerpagepriority]

Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{8cc29128-
   Queries value:
0b57-4a2b-a7b9-a74a70ba6fa1}[nameresource]
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6
                             50bbff5d15}[imagepath]
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
                                       5d15}[neverlowerpagepriority]
81f8-4b94-a608-6a
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6a50bbff5d15}[nameresource]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}[imagepath]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}[neverlowerpagepriority]
Queries\ value: HKLM \ system \ current control \ wdi \ diagnostic modules \ \{95c162b7-5b71-44f8-82e4-abfd3108f40f\} \ [namere source]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da-
b965-4fc3-8781-88dd50a6299d}[imagepath]
   Oueries value
                                        b965-4fc3-8781-88dd50a6299d}[neverlowerpagepriority]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da
   Oueries value
b965-4fc3-8781-88dd50a6299d}[nameresource]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
3f06-411b-9dd5-35bc5666ff3e}[imagepath]
                                        3f06-411b-9dd5-35bc5666ff3e}[neverlowerpagepriority]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
3f06-411b-9dd5-35bc56661
                                       ff3e}[nameresource]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
a6ca-48e0-a7c4-4cdd258439e2}[imagepath]
   Queries value:
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
\label{lem:a6ca-48e0-a7c4-4cdd258439e2} [neverlowerpagepriority] \\ Queries value: \\ HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules \end{4a59f0643-4bd} \\ \{a59f0643-4bd\} \\ \{a59f06
a6ca-48e0-a7c4-4
                             dd258439e2}[nameresource]
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
                                       a8c8}[imagepath]
a840-44a9-97b1
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
                             74fddaa8c8}[neverlowerpagepriority]
HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
a840-44a9-97b1-fb
   Queries value
                              4fddaa8c8}[nameresource]
a840-44a9-97b1-fb
   Queries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
60e9-4301-a338-b
                                       3e9}[imagepath]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
   Oueries value
60e9-4301-a338
                              b1c70b3e9}[neverlowerpagepriority]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\fb171ab1c-
60e9-4301-a338-beab1c70b3e9}[nameresource]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a068e}[imagepath]
   Oueries value
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a
                                       068e}[neverlowerpagepriority]
   Oueries value
                                        b736-48fb-84a0-5f0c389a068e}[nameresource]
                                        HKLM \ system \ current controls et \ control \ wdi \ diagnostic modules \ \{c0f51d84-diagnostic modules\} \ diagnostic \ modules \ diagn
11b9-4e74-b083-99f11ba2
                                       lb0a}[imagepath]
   Queries value
                                        11b9-4e74-b083-99f11ba2db0a}[neverlowerpagepriority]
                                        Oueries value
11b9-4e74-b083-99f11ba2
                                       lb0a}[nameresource]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}[imagepath]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}[neverlowerpagepriority]
Queries value: HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}[nameresource]
   Queries value:
                                        5be9-4f25-862e-485f1b1a6935}[imagepath]
                                        HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c8544339-
   Queries value
5be9-4f25-862e-485f1b1a6935}[neverlowerpagepriority]
Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{c8544339-
```

```
5be9-4f25-862e-485f1b1a6935}[nameresource]
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}[imagepath]
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
     Queries value:
6c33-4657-be74-4d0c32297ba4}[neverlowerpagepriority]

Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}[nameresource]

Queries value: HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}[imagepath]
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
     Queries value:
46c3-440e-bc65-dfa6a5094054}[neverlowerpagepriority]

Queries value: HKLM\system\currentcontrol\set\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}[nameresource]
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-
    Queries value:
3852-4952-b76b-23bb8e35d344}[imagepath]
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-
    Queries value
3852-4952-b76b-23bb8e35d344}[neverlowerpagepriority]
Queries value: HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-3852-4952-b76b-23bb8e35d344}[nameresource]
    Oueries value
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
3287-4e3f-af68-632c90f3ac95}[imagepath]
                                                                               HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
     Oueries value
3287-4e3f-af68-632c90f3ac95}[neverlowerpagepriority]
     Oueries value
                                                                               HKLM \verb|\system| current controls et \verb|\control| wdi \verb|\diagnostic modules| \{e80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae-te80cfaae
3287-4e3f-af68-632c90f3ac95}[nameresource]
                                                                              HKLM\system\currentcontrolset\control\wdi\config[servername]
HKLM\system\currentcontrolset\control[waittokillservicetimeout]
     Queries value
      Queries value:
     Oueries value
                                                                               HKLM\system\currentcontrolset\control\wmi\security[17fbab0b-1e4f-45f8-
91ed-c1c85bcf6e61]
      Queries value:
                                                                               HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
     Queries value:
HKCU\software\microsoft\windows\currentversion\radar[clresolutioninterval]
                                                                               HKCU\software\microsoft\windows\currentversion\radar[displayinterval]
     Queries value:
                                                                               HKCU\software\microsoft\windows\currentversion\radar[skipwatson]
     Queries value:
\label{thm:local} \begin{tabular}{ll} HKLM \end{tabular} when $$ \end{tabular} exclusion $$ \end{tab
     Oueries value:
                                                                               HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}[]
                                                                               HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
      Queries value
e212013ea917}\inprocserver32[inprocserver32]
     Queries value:
                                                                               HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\tinprocserver32[]
     Oueries value
                                                                               HKCR\clsid\{9ac9fhe1-e0a2-4ad6-b4ee-
e212013ea917}\inprocserver32[threadingmodel]
     Queries value
                                                                               HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]
                                                                               HKCR\clsid\{c90250f3-4d7d-4991-9b69-
     Queries value
a5c5bc1c2ae6}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\\c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[]
      Oueries value
                                                                               HKCR\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprocserver32[threadingmodel]
                                                                               HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
      Queries value:
      Queries value:
                                                                              HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}[]
HKCR\clsid\{603d3801-bd81-11d0-a3a5-
      Queries value
     Oueries value
00c04fd706ec}\inprocserv
                                                                            /er32[inprocserver32]
                                                                               HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[]
     Oueries value:
                                                                               HKCR\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32[threadingmodel]
     Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]

Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
                                                                               HKLM\system\currentcontrolset\services\rpceptmapper[objectname] HKLM\system\currentcontrolset\services\rpcss[objectname]
      Oueries value:
     Queries value:
      Queries value:
                                                                               HKLM\system\currentcontrolset\services\eventsystem[objectname]
     Queries value:
                                                                               HKLM\system\currentcontrolset\services\bits[objectname]
                                                                               HKLM\system\currentcontrolset\services\bits[imagepath]
HKLM\system\currentcontrolset\services\bits[wow64]
      Queries value:
      Oueries value:
                                                                               HKLM\system\currentcontrolset\services\bits[requiredprivileges]
      Queries value
     Oueries value
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues[capabilities]
     Oueries value:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues[configflags]
                                                                               HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
     Oueries value:
      Queries value
                                                                               HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\\\660b90c8-73a9-4b58-8cae-355b7f55341b\\inprocserver32[]
     Oueries value
                                                                               HKCR\clsid\{660b90c8-73a9-4b58-8cae
355b7f55341b}\inprocserver32[threadingmodel]
                                                                               \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the current version \end{tabular} for the constraint of t
     Queries value:
ui1
                                                                               HKCU\control panel\desktop[caretwidth]
HKCU\control panel\desktop[cursorblinkrate]
     Queries value
     Queries value:
      Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[alwaysshowmenus]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[alwaysshowmenus]
                                                                               HKCU\software\microsoft\internet explorer\toolbar[menuuserexpanded]
      Queries value:
     Oueries value:
                                                                               HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}[]
                                                                               HKCR\clsid\{f5a8b627-4d46-4d65-92f3
      Queries value
73626ae31971}\inprocserver32[inprocserver32]
     Queries value:
                                                                               HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprocserver32[]
     Oueries value
                                                                               HKCR\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprocserver32[threadingmodel]
\label{thm:hklm:software-microsoft-windows-current-version-explorer-command-store-shell-windows.status-bar[explorer-command-handler] \\
     Queries value
HKLM \ software \ microsoft \ windows \ current version \ explorer \ command store \ shell \ windows \ status \ ar [implied selection model] \ details \ d
     Queries value
\label{thm:hklm} \begin{tabular}{llll} HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows\cstatus\bar[folderhandler]]{thm:hklm} \end{tabular} \begin{tabular}{lllll} HKLM\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cstatus\cs
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[invokecommandonselection]
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[sendtoverb]
     Queries value
HKLM\software\microsoft\windows\currentyersion\explorer\commandstore\shell\windows.statusbar[opencontrolpanel]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ command store \ shell \ windows \ status bar [open control panel page] \ determined \ for the limit \ f
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[panevisibleproperty]
     Queries value:
```

```
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
                                                                                             HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}[]
        Queries value
       Queries value
                                                                                             HKCR\clsid\{b77b1cbf-e827-44a9-a33a-
 6ccfeeaa142a}\inprocser
                                                                                          er32[inprocserver32]
       Queries value:
                                                                                             HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprocserver32[]
       Queries value
                                                                                             HKCR\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprocser
                                                                                         ver32[threadingmodel]
HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]
       Queries value:
       Oueries value
                                                                                             HKCR\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[inprocserver32]
       Queries value
                                                                                             HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[]
                                                                                             HKCR\clsid\{76765b11-3f95-4af2-ac9d-
       Queries value
ea55d8994f1a}\inprocser
                                                                                          er32[threadingmodel]
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-
      Queries value
 e946b44c8dd5}[system.pr
                                                                                        oplist.statusbar]
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{26dc287c-6e3d-4bd3-
      Queries value
b2b0-6a26ba2e346d} 4]
                                                                                             HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}[]
       Queries value:
                                                                                             HKCR\clsid\{b8967f85-58ae-4f46-9fb2-
        Queries value
5d7904798f4b}\inprocserver32[inprocserver32]
                                                                                             HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprocserver32[]
       Queries value:
       Oueries value:
                                                                                             HKCR\clsid\{b8967f85-58ae-4f46-9fb2-
 5d7904798f4b}\inprocser
                                                                                           er32[threadingmodel]
       Oueries value
                                                                                             HKCR\clsid\{031e4825-7h94-4dc3-h131-e946h44c8dd5}[system_statusicons]
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{7a55582b-bd8c-4475-
       Queries value:
b94c-b87a388a7899} 1001
       Queries value
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}[system.librarylocationscount]
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{908696c7-8f87-44f2-
       Queries value
80ed-a8c1c6894575} 21
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[system.sync.itemstate]
       Queries value:
        Queries value
                                                                                             HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{7bd5533e-af15-44db
b8c8-bd6624e1d032} 251
       Queries value:
                                                                                             HKCU\control panel\desktop[smoothscroll]
       Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
       Oueries value:
\label{thm:cursoftware} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [list viewal phase lect] \end{tabular}
       Oueries value
\label{thm:cu} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [list view shadow] \end{tabular} \label{thm:current}
       Oueries value
Hk\L^{M}\system\currentcontrolset\control\system\currentcontrolset\control\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcontrol\system\currentcont\currentcontrol\system\currentcont\currentcont\currentcont\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\curr
       Queries value
HKLM \system \land current control set \land control \ set \land control
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14[timestamp]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00ab02a9ab10912b3b7f8c017a344c8d14[setid]
HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14[recent]
\label{thm:local_hklm} HKLMhsystem \controlset \control \control
       Oueries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0 00 07db c6^182fdc0875f0a76803e4a9848a8c1ea7[timestamp]
       Oueries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00[stride]
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00ab02a9ab10912b3b7f8c017a344c8d14\00[pixelformat]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00\ab02a9ab10912b3b7f8c017a344c8d14\00[colorbasis]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00[position.cx]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00ab02a9ab10912b3b7f8c017a344c8d14\00fposition.cvl
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\001flags1
       Queries value
HKLM \system \current control \system \current control \system \current \control \system \current \c
       Queries value:
HKLM \system \current control \system \current control \system \current \control \system \current \cu
       Queries value
Oueries value
Oueries value
HKLM \system \current control \system \current control \system \current \control \system \current \
       Oueries value
Oueries value
H\dot{\textbf{K}} \textbf{M} \textbf{System} \textbf{Current control set $\subset$ control \textbf{Spring} \textbf{Current} \textbf{Spring} \textbf{Spr
       Oueries value
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00^ab02a9ab10912b3b7f8c017a344c8d14\00\00[pixelrate]
      Oueries value
Oueries value
Oueries value
HKLM\software\microsoft\windows\currentversion\policies\explorer[notaskgrouping]
       Queries value
\label{local-observation} \mbox{\currentversion-explorer-advanced[taskbarglomlevel]} \mbox{\curre
       Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbaranimations]
       Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbarsmallicons]
HKLM\software\microsoft\windows\currentversion\explorer\advanced[taskbarsmallicons]
Queries value: HKLM\sys
b8e8-d92d736469be}[capabilities]
                                                                                             HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
       Queries value:
                                                                                             HKLM \ system \ current controls et \ enum \ swd \ printenum \ \{af023001-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e
b8e8-d92d736469be\} [configflags] \\ Queries value: HKLM\system\currentcontrol\set\control\devicecontainers \control\devicecontainers \control\devic
HKLM\system\currentcontrolset\control\devicecontainers\\\ 623cc954-8780-
       Queries value:
```

```
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en]
                                                                                               HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
Queries value: https://deachies.com/carchies/saceartes/carchies/saceartes/carchies/saceartes/carchies/saceartes/carchies/saceartes/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchies/carchie
b8e8-d92d736469be}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011[]
                                                                                               HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
       Queries value
b32c-cd2da77617c7}[capabilities]
       Queries value:
                                                                                               HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}[configflags]
                                                                                               HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
       Queries value
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en]

Queries value: HKLM\system\currentcontrol\set\control\devicecontainers\\623cc955-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[]
                                                                                               HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
       Queries value:
b32c-cd2da77617c7}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011[]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
                                                                                               HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d\\ shellfolder[attributes] \\ Queries value: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2\}[]
       Oueries value:
                                                                                               HKCR\clsid\{317d06e8-5f24-433d-bdf7-
 79ce68d8abc2}\inprocserver32[inprocserver32]
                                                                                               HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32[]
       Oueries value:
       Queries value:
                                                                                               HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-
Queries value: hkKCR\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[threadingmodel]
      Queries value:
 \label{thm:local_hamma} \begin{tabular}{ll} HKLM \software \microsoft \windows \current version \policies \nonenum \cite{Local_local_saea-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a2dd-1069-a
08002b30309d}1
       Queries value:
                                                                                               HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}[sortorderindex]
       Oueries value:
 HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders[suppressionpolicy]
      Oueries value
\label{thm:local_hamma} \begin{tabular}{ll} HKLM \label{thm:local_hamma} software \end{tabular} in the constraint of t
       Oueries value:
 1cc3-42a6-926c-e6a863f0e3ba}[suppressionpolicy]
Queries value: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}[]
        Oueries value:
                                                                                               HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprocserver32[inprocserver32]
       Queries value:
                                                                                              HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32[]
       Queries value:
 \label{thm:local-condition} HKLM \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\microsoft| my computer \verb|\namespace| delegate folders \verb|\scale= 1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.5786d3c-1.57866d3c-1.5
b075-49b9-88dd-029876e11c01}[suppressionpolicy]
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{9113a02d-
00a3-46b9-bc5f-9c04daddd5d7}[suppressionpolicy]
      Oueries value:
 \label{thm:local_ham} HKL \begin{tikzpicture}{ll} MKL \b
02f0-451e-9a26-ae317cfd7779}[suppressionpolicy]
Queries value: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-
Oueries value:
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[attributes]
       Queries value
                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[callforattributes]
HKLM \label{lem:hkk} In the latest and the latest
367a-4540-916b-f183c5093a4b}]

Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[foldervalueflags]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value
8d23b85255bf}\shellfolder[wantsfordisplay]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value
8d23b85255bf}\shellfolder[hidefolderverbs]
       Oueries value
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[usedrophandler]
       Oueries value
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[wantsforparsing]
Queries value: HKCR\clsid\\9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[queryforoverlay]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Queries value
8d23b85255bf}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\clsid\{9c73f
8d23b85255bf}\shellfolder[queryforinfotip]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Queries value
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[hideinwebview]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
Queries value: Inscrize (1907)

Rd23b82525bf}\shellfolder[hideondesktopperuser]

Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[wantsaliasednotifications]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Queries value:
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
Queries value: https://doi.org/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001
8d23b85255bf}\shellfolder[hasnavigationenum]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[enablethumbnails]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value
8d23b85255bf}\shellfolder[nodefaulttofs]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value:
8d23b85255bf}\shellfolder[parsedisplaynameneedsurl]
      Oueries value:
                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[blocknewfile]
                                                                                               HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value
8d23b85255bf}\shellfolder[noinitrequired]
```

```
Queries value
                                                         HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[saferootformta]
   Queries value:
 HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}]
                                                         HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32[]
   Queries value:
Queries value: HKCR\clsid\\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf\}\inprocserver32[loadwithoutcom]
   Queries value
                                                         HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf} {000214e6-0000-0000-c000-000000000046}}
0xffff1
                                                         HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[]
   Queries value
    Oueries value
                                                         HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[inprocserver32]
                                                         HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[threadingmodel]
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-7c88-d5291c64-
11e3-be65-806e6f6e6963}[generation]
   Queries value:
                                                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Oueries value
\label{thm:local} HKLM \software \microsoft \windows \current version \end{tens} is not represent the suppose of the suppose
   Oueries value
\label{thm:local_hamma} \begin{tabular}{ll} HKLM \software \microsoft \windows \current version \explorer \users libraries \names pace \delegate folders \cite{thm:local_hamma} \end{tabular}
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders\{896664f7-
12e1-490f-8782-c0835afd98fc}[suppressionpolicy]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.hideondesktop]
    Queries value:
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2-
b5d6-00c04fd918d0} 34]
HKLM\software\microsoft\windows\currentversion\explorer\hidedesktopicons\newstartpanel\[{condition:property}]{20d04fe0-property}
3aea-1069-a2d8-08002b30309d}]
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.namespaceclsid]
   Queries value:
                                                          HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2
b5d6-00c04fd918d0} 61
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}[system.ispinnedtonamespacetree]
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{5d76b67f-9b3d-44bb-
   Queries value
h6ae-25da4f638a671 21
   Queries value:
                                                         \label{thm:local-continuous} HKCU \software \mbox{$\operatorname{$\mathsf{MKCU}$ in $\mathsf{MKCU}$ in $\mathsf{MKCU}$ in $\mathsf{MKCU}$ in $\mathsf{MKCU}$ is $\mathsf{MKCU}$. The second of $\mathsf{MKCU}$ is $\mathsf{MKCU}$ is $\mathsf{MKCU}$ in $\mathsf{
3aea-1069-a2d8-08002b30309d}\defaulticon[]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\defaulticon[openicon]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}[]
                                                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
   Queries value:
     Queries value:
                                                         HKLM\system\currentcontrolset\services\bits[type]
   Queries value:
                                                         HKLM\system\currentcontrolset\services\bits[start]
    Queries value:
                                                          HKLM\system\currentcontrolset\services\bits[errorcontrol]
                                                         HKLM\system\currentcontrolset\services\bits[tag]
   Oueries value:
                                                          HKLM\system\currentcontrolset\services\bits[dependonservice]
    Queries value
   Oueries value:
                                                         HKLM\system\currentcontrolset\services\bits[dependongroup]
    Queries value:
                                                          HKLM\system\currentcontrolset\services\bits[group]
    Oueries value:
                                                         HKLM\system\currentcontrolset\services\http[objectname]
                                                          HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
    Queries value:
                                                         HKLM\system\currentcontrolset\services\ssdpsrv[imagepath]
   Oueries value:
                                                          HKLM\system\currentcontrolset\services\ssdpsrv[wow64]
    Queries value:
                                                         HKLM\system\currentcontrolset\services\ssdpsrv[requiredprivileges]
HKLM\system\currentcontrolset\services\sppsvc[objectname]
    Oueries value
    Queries value:
                                                         HKLM\system\currentcontrolset\services\sppsvc[imagepath]
HKLM\system\currentcontrolset\services\sppsvc[wow64]
    Queries value:
    Queries value:
    Queries value:
                                                         HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
                                                         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
   Queries value:
20[profileimagepath]
   Oueries value
                                                         HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
                                                         HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
   Oueries value
shell folders[local appdata]
                                                         HKLM\system\currentcontrolset\services\sppsvc[environment]
   Oueries value:
                                                          HKLM\system\currentcontrolset\services\sppsvc[startprotected]
    Queries value:
   Oueries value:
                                                         HKLM\software\microsoft\windows
nt\currentversion\compatibility32[sppsvc]
   Oueries value:
                                                         Queries value:
a5f9-f2bdfea0f1561
                                                         HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]
   Queries value:
                                                      HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
ver32[inprocserver32]
   Oueries value
323e85a1ce84}\inprocser
   Queries value
                                                         HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]
                                                         HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
   Queries value
                                                        er32[threadingmodel]
323e85a1ce84}\inprocser
                                                         HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-
   Oueries value
8539-9230a44081a5]
   Oueries value
                                                         HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-
809b-2a87b70881f8]
                                                         HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-
   Oueries value
833b-323e85a1ce84]
   Oueries value
                                                         HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Oueries value
                                                         HKLM\software\policies\microsoft\internet
explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\internet explorer\security[disablefixsecuritysettings]
   Queries value:
                                                         HKLM\software\microsoft\internet
explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action 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
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]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\action
```

```
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-
  Queries value
{\tt 0e34774a413d} \verb+\inprocserver32[threading model]
                             HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:
  Oueries value
                             9270-3b2691a0a394]
Queries value:
86ba-948b70416220]
                             HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-
                             \label{thm:local-problem} \begin{tabular}{ll} HKLM\software\mbox{\tt microsoft\windows\windows} & error reporting[disabled] \\ HKCU\software\mbox{\tt microsoft\windows\windows} & error reporting[disabled] \\ \end{tabular}
  Oueries value
  Queries value:
  Queries value
                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
                             HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
HKCR\clsid\{88d96a05-f192-11d4-a65f-
  Queries value
0040963251e5}\inprocser
                             er32[inprocserver32]
                             HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value:
                              HKCR\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.100[checksetting]
                             HKCU\software\microsoft\windows\windows error
  Queries value:
reporting[lastque
Queries value:
                      enestertimel
                             HKLM\software\microsoft\windows\windows error
reporting[queuepesterinterval]
                             HKCU\software\microsoft\windows\windows error
  Queries value:
reporting[queuepesterinterval]
                             HKCU\software\microsoft\windows\currentversion\action
  Queries value
Queries value
                             HKCR\clsid\{c8e6f269-b90a-4053-a3be
499afcec98c4}\inprocserver32[inprocserver32]
  Queries value:
                             \label{localization} HKCR \verb|\clsid|{c8e6f269-b90a-4053-a3be-499afcec98c4} \verb|\inprocserver32[]|
  Queries value
                             HKCR\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32[threadingmodel]
  Oueries value
Oueries value
                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0[checksetting]
  Oueries value:
                             HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
                             HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}[]
  Queries value:
  Oueries value
                             HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[inprocserver32]
  Queries value:
                             HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
HKCR\clsid\{088e8dfb-2464-4c21-bad2-
  Queries value
                            /er32[inprocserver32]
HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[]
f0aa6db5d4bc}\inprocser
  Queries value:
                             HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[threadingmodel]
                             HKCR\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprocserver32[threadingmodel]
  Queries value:
                             HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
  Oueries value:
                             HKLM\software\policies\microsoft\windows\system[enablesmartscreen]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer[smartscreenenabled]
  Queries value:
                             {\tt HKCU \ } software \verb|\microsoft| windows \verb|\currentversion| action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
                             HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
  Queries value:
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[inprocserver32]
  Queries value
                             HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
                             HKCR\clsid\{a4a1a128-768f-41e0-bf75-
  Queries value
e4fddd701cba}\inprocse
                             er32[threadingmodel]
                             HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}[]
  Queries value:
  Queries value
                             HKCR\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprocserver32[inprocserver32]
                             HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[]
HKCR\clsid\{d26de5c1-c061-43f7-9c40-
  Queries value:
  Oueries value
7517526cf1c1}\inprocserver32[threadingmodel]
  Oueries value
\label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| startup notify [enable startup appnotification] \end{tabular}
  Oueries value
                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting]
                             HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018\}.check.100[checksetting]
                            HKCU\software\microsoft\windows\currentversion\action 42fa-414c-b8aa-eee2c8202018}.check.101[checksetting]
  Oueries value
center\checks\{01979c6a-
\label{lem:queries} Queries \ value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881\}[lastknownstate]}
Queries value: 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]
                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78\.check.101[checksetting]
                             HKCU\software\microsoft\windows\currentversion\action
  Queries value
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a\}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
  Queries value:
center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017\}.check.800[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
  Queries value
center \verb|\providers| eventlog \verb|\final 134ea 407-755d-4a 93-b8a6-f290cd 155023 \} [lastknown state] \\
                             HKCU\software\microsoft\windows\currentversion\action
  Queries value
center\checks\{134ea407-755d-4a93-b8a6-f290cd155023\}.check.8001[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\providers
                      ventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}[lastknownstate]
                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100[checksetting]
                             HKCU\software\microsoft\windows\currentversion\action
  Oueries value
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100[checksetting]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100[checksetting]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\action
center \providers \end{\{2374911b-b114-42fe-900d-54f95fee92e5\}[lastknown state]}
```

HKCU\software\microsoft\windows\currentversion\action

center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100[checksetting]

```
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139\}.check.8010[checksetting]
       Oueries value
                                                                                                            HKCU\software\microsoft\windows\currentversion\action
                                                                                                        og\{aa4c798d-d91b-4b07-a013-787f5803d6fc}[lastknownstate]
 center\provide
                                                                           HKCU\software\microsoft\windows\currentversion\action
4c798d-d91b-4b07-a013-787f5803d6fc}.check.100[checksetting]
       Oueries value
center\checks\{aa-
\label{lem:lem:queries} Queries \ value: \\ HKLM\software\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbox{\software}\mbo
       Oueries value
                                                                                                            HKLM\software\microsoft\windo
nt\currentversion\softwareprotectionplatform[keeprunningthresholdmins]
       Queries value
                                                                                                            HKLM\system\currentcontrolset\services\wsearch[objectname]
HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
        Queries value
       Queries value
                                                                                                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                                                                                                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
                                                                                                            HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform[tokenstore]
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1[]
       Queries value
        Queries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10[]
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11[]
        Queries value
        Oueries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12[]
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13[]
        Queries value:
       Oueries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14[]
        Queries value:
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15[]
        Oueries value
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16[]
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17[]
        Queries value:
        Oueries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18[]
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19[]
        Queries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2[]
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20[]
        Oueries value
        Queries value:
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21[]
         Queries value
                                                                                                            HKLM\system\wpa\8decOaf1-0341-4b93-85cd-72606c2df94c-6p-22[]
        Queries value:
        Queries value
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23[]
       Queries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24[]
        Queries value
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25[]
        Oueries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26[]
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27[]
        Queries value
       Oueries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28[]
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29[]
        Queries value:
        Oueries value
                                                                                                            HKLM \ system \ wpa \ 8 dec 0 af 1 - 0341 - 4b 93 - 85 cd - 72606 c 2d f 94 c - 6p - 3[]
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30[]
        Queries value:
        Oueries value:
                                                                                                            HKLM \ system \ wpa \ 8 dec 0 af 1 - 0 3 4 1 - 4 b 9 3 - 85 cd - 72606 c 2 df 9 4 c - 6 p - 31 [] \\
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32[]
        Queries value:
        Queries value:
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33[]
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4[]
        Queries value:
        Oueries value
                                                                                                            HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5[]
                                                                                                            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[1
        Queries value:
                                                                                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9[]
       Oueries value:
                                                                                                            HKLM\software\microsoft\windows
 \verb| nt/currentversion/software protection platform/plugins/modules/179b8a65-b0f6-41d9-acea-like the following of the properties of the pr
 12006ef9b32a[manifestfile]
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
\verb|nt\currentversion\software protection platform \verb|plugins\modules\179b8a65-b0f6-41d9-acea-leady and the control of the cont
 12006ef9b32a[pluginfile]
       Oueries value
                                                                                                           HKIM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| modules \verb|\c42d83ff-5958-4af4-a0dd-4| and the control of the 
ba02fed39662[manifestfile]
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
 \verb|nt/currentversion/software| protection platform \verb|plugins| modules \verb|c42d83ff-5958-4af4-a0dd-def| with the control of the 
ba02fed39662[pluginfile]
       Queries value
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0fisservicel
                                                                                                            HKLM\software\microsoft\windows
\label{lem:ntcurrentversion} nt\currentversion\software protection platform\plugins\objects\mbox{\sc msft:rm/algorithm/flags/1.0[moduleid]} \\ Queries\ value: HKLM\software\mbox{\sc microsoft\windows}
\label{lem:ntcurrentversion} nt current version software protection platform \ plugins \ objects \ msft: rm/algorithm/hwid/4.0 \ [moduleid] Queries value: HKLM \ software \ microsoft \ windows
\label{lem:nt-current-weight-decomposition} $$ nt\circ \end{substitute} $$ nt\circ \end{substitute} $$ nt\circ \end{substitute} $$ Queries value: $$ HKLM\software\microsoft\windows $$ HKLM\software\microsoft\windows $$ nt\circ \end{substitute} $$ nt\circ \end{subs
nt\currentversio
                                                                                  softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
                                                                                                            HKLM\software\microsoft\windows
       Queries value
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[moduleid] Queries value: HKLM\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/pkey/detect[moduleid]| and the platform of the 
                                                                                                            HKLM\software\microsoft\windows
       Queries value
                                                                                                            reprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[moduleid]
nt\currentversion\softw
                                                                                                            HKLM\software\microsoft\windows
       Oueries value
                                                                                                            reprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
nt\currentversio
       Oueries value
                                                                                                            HKLM\software\microsoft\window
                                                                                                            reprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[moduleid]
nt\currentversion\softw
       Oueries value
                                                                                                            HKLM\software\microsoft\window
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/action/kernel/1.0[moduleid]| and the software protection platform objects \verb|\msft:spp/action/kernel/1.0[moduleid]| and the software protection platform objects \verb|\msft:spp/action/kernel/1.0[moduleid]| and the software protection platform objects obje
       Oueries value
                                                                                                            HKLM\software\microsoft\window
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/action/reeval/1.0[moduleid]| and the properties of t
       Oueries value
                                                                                                            HKI M\software\microsoft\windov
nt \verb|`currentversion'| software protection platform \verb| plugins | objects | msft: spp/action/vlactivate/1.0[moduleid] | objects | msft: spp/action/vlactivate/1.0[moduleid] | objects | msft: spp/action/vlactivate/1.0[moduleid] | objects | objects
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[moduleid]
       Queries value
                                                                                                            HKLM\software\microsoft\window
Queries value
                                                                                                            HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[moduleid]
       Queries value
                                                                                                            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[moduleid]
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows
nt \verb|currentversion| software protection platform \verb|plugins| objects| msft:spp/license acquisition/payload handler/pkc/1.0[moduleid] and the properties of the properties of
       Queries value:
                                                                                                            HKLM\software\microsoft\windows
Queries value
                                                                                                            HKLM\software\microsoft\window
```

HKCU\software\microsoft\windows\currentversion\action

Queries value

```
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[moduleid]
\label{lem:ntcurrent} $$ nt\current version\software protection platform \plugins \objects\msft: spp/license acquisition/sequence/1.0[moduleid] $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:spp/statecollector/pkey[moduleid]| and the software protection platform objects \verb|\msft:spp/statecollector/pkey[moduleid]| and the software protection platform objects \verb|\msft:spp/statecollector/pkey[moduleid]| and the software protection platform objects 
                                                        HKLM\software\microsoft\windows
   Queries value
\label{lem:nt-current-continuous} $$ nt\currentversion\softwareprotection platform \plugins \objects\mbox{\sc spp/taskscheduler/1.0[moduleid]} $$ Queries value: $$ HKLM\software\mbox{\sc microsoft}\windows $$ $$
nt\currentversion
                                         softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
                                                        HKLM\software\microsoft\windows
   Queries value
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[moduleid]
Queries value: HKLM\software\microsoft\windows
                                                       reprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[moduleid]
nt\currentversi
                                                        HKLM\software\microsoft\windows
   Queries value
                                                        reprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[isservice]
nt\currentversi
   Queries value
HKLM\system\cu
                                           controlset\services\lanmanworkstation\parameters[rpccachetimeout]
   Oueries value
                                                        HKLM\software\microsoft\windows
                                                       reprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[isservice]
nt\currentversion
   Queries value
                                                        HKLM\software\microsoft\window
                                                        reprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[isservice]
nt\currentversion
   Oueries value
                                                        HKLM\software\microsoft\window
nt\currentversion\softwa
                                                       reprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[isservice]
   Oueries value
                                                        HKI M\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[isservice]
                                                        HKLM\software\microsoft\window
   Oueries value
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[isservice]
   Oueries value
                                                        HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[isservice]
   Queries value
                                                        HKLM\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[isservice]
                                                        HKLM\software\microsoft\windov
nt \verb|\colored | the form \verb|\colored | the 
   Queries value
                                                        HKLM\software\microsoft\windows
\label{lem:nt-current-version-software-protection-plugins-objects-msft:rm/algorithm/volume/1.0[isservice] \\ Queries value: HKLM\software\microsoft\windows
\label{lem:ntcurrent} $$nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[isservice] $$Queries\value: HKLM\software\microsoft\windows
                                        \softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[isservice]
HKLM\software\microsoft\windows
nt\currentversion
   Queries value
\label{lem:nt-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-curren
                                                      ireprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[isservice]
HKLM\software\microsoft\windows
nt\currentversio
   Queries value
nt\currentversion
                                                       reprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[isservice]
HKLM\software\microsoft\windows
   Queries value
nt\currentversi
                                                        reprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0[isservice]
   Queries value
                                                        HKLM\software\microsoft\windows
                                                        reprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[isservice]
nt\currentversi
   Queries value
                                                        HKLM\software\microsoft\window
nt\currentversio
                                                        reprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[isservice]
   Oueries value
                                                        HKLM\software\microsoft\window
                                                        reprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[isservice]
nt\currentversio
   Oueries value
                                                        HKLM\software\microsoft\window
nt\currentversion\softwa
                                                       reprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[isservice]
   Oueries value
                                                        HKLM\software\microsoft\window
\verb|nt| current version | software protection platform \verb|plugins| objects | msft:spp/licenseacquisition/payload handler/pkc/1.0[isservice]| | the protection of the protection
   Oueries value
                                                        HKI M\software\microsoft\windov
Queries value
                                                        HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[isservice]
                                                        HKLM\software\microsoft\window
   Queries value
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[isservice]
                                                        HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey[isservice]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[isservice]
                                                        HKLM\software\microsoft\windows
   Queries value
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0fisservicel
                                                        HKLM\software\microsoft\windows
\label{lem:nt-current-version-software-protection-platform-plugins-objects-msft:spp/volume/services/kms/activationinfo/1.0[isservice] \\ Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                                                        Oueries value:
    Queries value:
   Oueries value
                                                        HKCU\software\microsoft\windo
nt\currentversion\softwareprotectionplatform[kmshostconfig]
   Oueries value
                                                        HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform[enabletestvolumeintervals]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[vlactivationinterval]
Queries value: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[vlrenewalinterval]
                                                        HKLM\software\microsoft\windo
   Queries value
nt\currentversion\softwareprotectionplatform[actionlist]
   Queries value
HKLM\software\microsoft\windows\currentversion\sidebyside[publisherpolicychangetime]
   Queries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[cachestore]
                                                        HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
   Queries value:
                                                        Oueries value:
    Queries value:
   Oueries value:
                                                        Queries value
\label{thm:hklm} \begin{tabular}{ll} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MNsystem \current control set \enum \pci \ven\_8086\&dev\_1237\&subsys\_00000008rev\_02\label{thm:hklm} 23.8267a616a\&1\&00[hardwareid] \end{tabular}
Queries value
HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0fhardwareidl
   Oueries value:
    Queries value
HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0fcompatibleids1
   Queries value:
                                                        HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[hardwareid]
   Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[compatibleids]
   Queries value:
                                                        HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[hardwareid]
    Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[compatibleids]
   Queries value:
                                                        HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[hardwareid]
```

```
Queries value
HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[compatibleids]
 Oueries value
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1fhardwareid
 Oueries value:
\label{local_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\enum\line(1) and the local properties of the local pr
 Queries value:
Queries value:
                               HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[hardwareid]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[compatibleids]
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 7111&subsys 00000000&rev 01\3&267a616a&1&09[hardwareid]
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 7111&subsys 00000000&rev 01\3&267a616a&1&09[compatibleids]
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[hardwareid]
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[compatibleids]
HKLM\system\currentcontrolset\enum\ide\diskhitachi
                                                                                                       1.0.7.3 \5&34baf594&0&0.0.0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi
                                                                                                      1 0 7 3 \5&34haf594&0&0 0 O[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[hardwareid]
  Queries value
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[compatibleids]
 Queries value:
                              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[licstatusarray]
                               HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\softwareprotectionplatform[policyvaluesarray]
 Queries value:
                               HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[hasooberun]
  Queries value:
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}[]
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value:
  Oueries value:
                               HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
                              \label{thm:local_hammon} HKCU\control\ panel\ international[scurrency override] \\ HKLM\software\mbox{\em microsoft}\windows
  Oueries value:
  Queries value:
nt\currentversion\softwareprotectionplatform[servicesessionid]
Queries value: HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}[]
  Oueries value
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value
                               HKCR\clsid\{88d96a08-f192-11d4-a65f-
  Queries value
0040963251e5}\inprocserver32[threadingmodel]
                               HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\softwareprotectionplatform[logcontext]
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}{[]
  Oueries value:
  Queries value
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[inprocserver32]
  Queries value:
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
  Oueries value:
                               HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[threadingmodel]
  Oueries value:
                               HKLM\system\currentcontrolset\control\productoptions[productpolicy]
  Sets/Creates value:
                               HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel] Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[]
                               HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34[]
  Sets/Creates value:
  Value changes:
                               HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
  Value changes:
Value changes:
Value changes
Value changes
Value changes
Value changes
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000005 \ [packed catalog item]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000[packedcatalogitem]
 Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000001fpackedcatalogitem
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\00000000010fpackedcatalogitem1
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\000000000009fpackedcatalogitem1
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem] Value changes:
HKLM \system \correct control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \\64 \colono 0000000005 \cite[packed catalogitem]
  Value changes:
Value changes:
HKLM \system \correct control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \\64 \colono 0000000003 \[packed catalog item]
  Value changes
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
 Value changes
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\000000000001[packedcatalogitem]
  Value changes
\label{local-holes} HKLM \system \current controls et\services \winsock 2\parameters \names pace\_catalog 5\catalog\_entries \noone0000000005[library path] \end{subarray}.
 Value changes
HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalogS \catalog\_entries \colono 0000000000004 \[library path]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
```

Value changes:

Value changes: Value changes: HKLM\system\currentcontrolset\services\browser[start]
HKLM\system\currentcontrolset\services\policyagent[start]

Value changes: HKCU\software\microsoft\internet explorer\toolbar\shellbrowser[itbar7layout]

Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.106[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting] Value changes: HKCU\software\microsoft\windows\currentversion\action

Value changes. HKLM\software\microsoft\windows

HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[servicesessionid] Value changes: HKLM\software\microsoft\windows value changes: IRLEM\software\microsoft\windows

Value changes: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform[actionlist]