Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID: 823 Risk Level: 10

2016-05-18 10:42:17 (UTC) Date Processed:

Processing Time: 62.92 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"

Sample ID 3329 Type: basic Owner: admin

Label: 26ec828da6d2651f90c74cb275b800cc

Date Added 2016-05-18 10:30:51 (UTC) PE32:win32:gui File Type:

File Size:

184320 bytes 26ec828da6d2651f90c74cb275b800cc MD5:

SHA256:

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

Creates malicious events: ZeroAccess [Rootkit]
Changes Winsock providers

3 Connects to local host

4 Reads process memory

3 Long sleep detected

5 Installs service

Process/Thread Events

Creates process: C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe

["C:\windows\temp\26ec828da6d2651f90c74cb275b800cc.exe"]
Creates process: C:\Windows\system32\rundl132.exe [C:\Windows\system32\rundl132.exe Creates process:

bfe.dll,BfeOnServiceStartTypeChange]
Creates process: C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe] PID:144 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe PID:3064 C:\Windows\SysW0W64\calc.exe Reads from process:

Reads from process:

PID:144 C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe Writes to process: PID:2024 C:\Windows\explorer.exe Writes to process:

Writes to process:

PID:484 C:\Windows\System32\services.exe C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe Terminates process:

Terminates process: C:\Windows\System32\rundll32.exe 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

Creates event: \Se 2F90-6754-8374-21D4DAB28CC1} \Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{0C5AB9CD-

\BaseNamedObjects\\BaseNamedObjects\\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D773 \Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{A3D35150-

Creates event 6823-4462-8C6E-7417FF841D78}

Creates event: \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

File System Events

Creates C:\Program Files\Windows Defender\en-US: C:\Program Files\Windows Defender\EppManifest.dll:! Creates: :\Program Files\Windows Defender\MpAsDesc.dll:! Creates C:\Program Files\Windows Defender\MpClient.dll:!

\Program Files\Windows Defender\MpCmdRun.exe:! Creates C:\Program Files\Windows Defender\MpCommu.dll:!
C:\Program Files\Windows Defender\MpEvMsg.dll:! Creates Creates

C:\Program Files\Windows Defender\MpOAV.dll:!
C:\Program Files\Windows Defender\MpRtp.dll:! Creates Creates :\Program Files\Windows Defender\MpSvc.dll:! :\Program Files\Windows Defender\MpTpmAtt.dll:! Creates Creates: Creates: \Program Files\Windows Defender\MpUtil.dll:! \Program Files\Windows Defender\mpuxhostproxy.dll:! :\Program Files\Windows Defender\MpUXSrv.exe: :\Program Files\Windows Defender\MSASCui.exe: Creates

Creates :\Program Files\Windows Defender\MsMpCom.dll:! :\Program Files\Windows Defender\MsMpEng.exe:! Creates: Creates \Program Files\Windows Defender\MsMpLics.dll:! \Program Files\Windows Defender\MsMpRes.dll:! Creates

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

\\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3 Creates Creates C:\\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3\L C:\\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3\U Creates \\$Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3\@\\Recycle.Bin\S-1-5-18\\$915369118a4888a39e2f92dbd118adb3\n Creates Creates: Creates C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001

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

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

1001\\$915369118a4888a39e2f92dbd118adb3\L

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

1001\\$915369118a4888a39e2f92dbd118adb3\U Creates

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\ Creates C:GAC MSTL

C:\\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-Creates 1001\\$T5D1DD46B

C:\Windows\assemblv\GAG Creates

```
Creates
                                  C:GAC 32
   Creates
                                   C:GAC_64
  Creates
                                  C:\Windows\assembly\GAC 64\Desktop.ini
                                      \Windows\assembly\GAC_32\Desktop.ini
   Creates:
                                  C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
  Creates
                                      \Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles
  Creates
  Creates:
                                      \label{local} $$ \S Admin\AppData\Local\Microsoft\Windows\WER\ERC $$ Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC\S $$ atecache.lock $$
  Creates
                                      \Windows\System32\spp\store\data.dat.tmp
\Windows\Prefetch\26EC828DA6D2651F90C74CB275B80-7FC87F1F.pf
  Opens
  Opens:
                                  C:\Windows
                                      \Windows\System32\wow64.dll
  Opens
                                  C:\Windows\SysWOW64
C:\Windows\SysWOW64\apphelp.dll
   Opens:
  Opens:
                                      \Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
                                  C:\Windows\SysWOW64\ntdll.dll
  Opens
   Opens:
                                      \Windows\SysWOW64\kernel32.dll
  Opens
                                  C:\Windows\SysWOW64\KernelBase.dll
   Opens
                                      \Windows\apppatch\sysmain.sdb
  Opens:
                                  C:\Windows\SysWOW64\d3d8.dll
C:\Windows\SysWOW64\opengl32.dll
   Opens
  Opens:
                                  C:\Windows\SysWOW64\version.dll
                                      \Windows\SysWOW64\d3d8thk.dll
  Opens
  Opens:
                                  C:\Windows\SvsWOW64\dwmapi.dll
  Opens:
                                      \Windows\SysWOW64\sechost.dll
                                  C:\Windows\SysWOW64\glu32.dll
C:\Windows\SysWOW64\ddraw.dll
   Opens:
  Opens
                                  C:\Windows\SysWOW64\dciman32.dll
C:\Windows\SysWOW64\gdi32.dll
  Opens:
  Opens:
                                  C:\Windows\SysWOW64\user32.dll
C:\Windows\SysWOW64\msvcrt.dll
   Opens:
  Opens
                                  C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Windows\SysWOW64\cryptbase.dll
C:\Windows\SysWOW64\sspicli.dll
   Opens
  Opens:
   Opens:
                                  C:\Windows\SysWOW64\rpcrt4.dll
C:\Windows\SysWOW64\advapi32.dll
  Opens
   Opens
  Opens:
                                  C:\Windows\SvsWOW64\imm32.dll
                                      \Windows\SysWOW64\msctf.dll
   Opens:
                                  C:\Windows\SvsWOW64\mscat32.dll
  Opens:
                                      \Windows\SysWOW64\msasn1.dll
   Opens:
                                  C:\Windows\SysWOW64\crypt32.dll
C:\Windows\SysWOW64\wintrust.dll
  Opens:
  Opens:
  Opens:
                                  C:\Windows\Temp
  Opens:
   Opens:
                                  C:\Windows\System32\ntdll.dll
C:\Windows\System32\wow64win.dll
  Opens
                                  C:\Windows\System32\wow64cpu.dll
C:\Windows\System32\kernel32.dll
   Opens:
  Opens:
   Opens:
                                      \Windows\System32\user32.dll
                                     \Windows\SysWOW64\untfs.dll
  Opens
   Opens
                                     :\Windows\SysWOW64\cabinet.dll
:\Windows\SysWOW64\ws2_32.dll
  Opens:
                                      \Windows\SysWOW64\nsi.dll
   Opens:
  Opens:
                                  C:\Windows\Globalization\Sorting\SortDefault.nls
   Opens:
                                      \Windows\SysWOW64\mswsock.dll
  Opens:
                                  C:\Windows\SysWOW64\cryptsp.dll
C:\Windows\SysWOW64\rsaenh.dll
  Opens
  Opens
                                      \Program Files\Windows Defender
                                      \Program Files\Windows Defender\en-US
  Opens
                                     :\Program Files\Windows Defender\EppManifest.dll
:\Program Files\Windows Defender\MpAsDesc.dll
  Opens:
  Opens
                                     \Program Files\Windows Defender\MpClient.dll
\Program Files\Windows Defender\MpCmdRun.exe
  Opens:
  Opens:
                                     Opens:
  Opens
                                      \Program Files\Windows Defender\MpOAV.dll
\Program Files\Windows Defender\MpRtp.dll
  Opens:
                                      \Program Files\Windows Defender\MpSvc.dll
\Program Files\Windows Defender\MpTpmAtt.dll
   Opens:
  Opens:
                                      \Program Files\Windows Defender\MpUtil.dll
   Opens:
                                  C:\Program Files\Windows Defender\mpuxhostproxy.dll
  Opens:
                                      \Program Files\Windows Defender\MpUXSrv.exe
   Opens:
  Opens:
                                      \Program Files\Windows Defender\MSASCui.exe
  Opens:
                                      \Program Files\Windows Defender\MsMpCom.dll
  Opens:
Opens:
                                     :\Program Files\Windows Defender\MsMpEng.exe
                                      \Program Files\Windows Defender\MsMpLics.dll
                                     \Program Files\Windows Defender\MsMpRes.dll
\Program Files\Microsoft Security Client
  Opens:
  Opens:
Opens: C:\Program Files\microsort Security Client
Opens: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
Opens: C:\Windows\assembly
Opens: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\n
                                  C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001
C:\Windows\System32\mswsock.dll
  Opens
                                  C:\Windows\assembly\GAC_32\Desktop.ini
C:\Windows\assembly\GAC_64\Desktop.ini
C:\Windows\System32\cryptsp.dll
  Opens:
  Opens:
   Opens:
  Opens:
                                      \Windows\Svstem32\rsaenh.dll
                                      \$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@\\Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\U\\windows\System32\rundl132.exe
   Opens:
  Opens:
  Opens
  Opens:
                                      \Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
                                      \Windows\System32
  Opens
   Opens:
                                  C:\Windows\System32\en-US\rundll32.exe.mui
C:\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:
                                  C:\Windows\System32\dnsapi.dll
C:\Windows\System32\sechost.dll
  Opens
  Opens:
                                   C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\@
                                  C:\Users\desktop.ini
  Opens:
   Opens:
                                  C:\Users
                                      \Users\Admin
   Opens:
  Opens:
                                  C:\Users\Admin\AppData
   Opens:
                                  C:\Users\Admin\AppData\Roaming
                                  C:\Users\Admin\AppData\Roaming\Microsoft\desktop.ini
   Opens
   Opens
                                  C:\Users\Admin\AppData\Roaming\Microsoft
```

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows
     Opens
                                                                             \Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
      Opens:
                                                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries
C:\Users\Admin\Desktop\desktop.ini
     Opens:
      Opens:
     Opens:
                                                                      C:\Users\Public\desktop.ini
                                                                      C:\Users\Public
     Opens:
     Opens:
                                                                      C:\Users\Public\Desktop\desktop.ini
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
                                                                      C:\Windows\System32\wscinterop.dll
     Opens:
                                                                      C:\Windows\System32\wscapi.dll
C:\Windows\System32\wscui.cpl
     Opens:
     Opens:
                                                                      C:\Windows\System32\wscinterop.dll.123.Manifest
C:\Windows\System32\en-US\wscui.cpl.mui
     Opens:
     Opens:
                                                                       C:\Windows\System32\werconcpl.dll
      Opens:
                                                                      C:\Windows\System32\wer.dll
     Opens:
      Opens:
                                                                            :\Windows\System32\framedynos.dll
                                                                      C:\Windows\System32\wercplsupport.dll
     Opens:
      Opens:
                                                                             \Windows\System32\msxml6.dll
     Opens:
                                                                       C: \windows\System 32\msxml6r.dl1 \\ C: \users\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive \\
     Opens:
                                                                      C:\ProgramData\Microsoft\Windows\WER\ReportArchive
     Opens:
                                                                             \Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
                                                                      C:\Windows\System32\hcproviders.dll
C:\Windows\WinSxS\amd64_microsoft.windows.common-
     Opens:
     Opens
C:\Program Files\Internet Explorer\ieproxy.dll
C:\Windows\System32\en-US\ActionCenter.dll.mui
     Opens:
     Opens:
                                                                      C:\Windows\System32\Actioncenter.dll.3.Manifest
C:\Windows\ServiceProfiles
      Opens:
     Opens:
                                                                      C:\Windows\System32\sppsvc.exe
C:\Windows\System32\sppsvc.exe
      Opens
     Opens:
                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE}\Adobe-Flash-For-Windows-Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-
Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
Opens: OCC04FC295EE}\Microsoft-Hyper-V-Management-Clients-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-
net-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-
Package~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-minkernel-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-1101-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Hyper-V-Server-Drivers-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim 100c04FC295EE \\ \sim 100c04FC2
US~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-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Anytime-Upgrade-Package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3856ad364e35-amd64-endown-package-31bf3866ad364e35-amd64-endown-package-31bf3866ad364e35-amd64-endown-package-31bf3866ad364e35-amd64-endown-package-31bf3866ad364e35-amd64-endown-package-31bf3866ad364e35-amd64-endown-package-31bf3866ad364e35-amd64-endown-package-31bf3866ad364e36-amd64-endown-package-31bf3866ad364e36-amd64-endown-package-31bf3866ad364e36-amd64-endown-package-31bf3866ad364e36-amd64-endown-package-31bf3866ad364e36-amd64-endown-package-31bf3866ad364e36-amd64-endown-package-31bf3866ad364e36-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-a
US~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
     Opens:
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-Package-31bf3856ad364e35-amd64~en-
US~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                      C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-ApisetNamespace-Base-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim ende
 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
                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
```

```
Opens
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\f750E6C3-38EE-11D1-85E5-
00C04FC295E}\Microsoft-Windows-ApisetNamespace-Com-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\f750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-Mincore-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endownorm 
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-
       Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           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-
       Opens:
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-
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-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-ApisetNamespace-Windows-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endows-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endows-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endows-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endows-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endows-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endows-Package \\ \sim endows-Packag
US~6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-ApisetNamespace-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Windows-W
Package-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-AvCore-
Package-31bf3856ad364e35-amd64~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-Base-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ApisetNamespace-WOW64-Com-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim n-Package \\ 
US~6.2.9200.16384.cat
Opens:
                                                                                           C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EB}\Microsoft-Windows-ApisetNamespace-W0W64-Com-
Package-31bf3856ad364e35-amd64--6.2.9200.16384.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-W0W64-Mincore-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-ApisetNamespace-WOW64-Minio-Package \sim 31bf3856ad364e35 \sim amd64 \sim en-100c04 \sim 100c04 
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.1b384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-Minkernel-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package~31bf3856ad364e35~amd64~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ApisetNamespace-W0W64-Windows-Package-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           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
US~6.2.9200.16384.cat
      Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-BLB-Client-Package-31bf3856ad364e35-amd64-en-defined by the statement of the statement o
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                 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-
       Opens:
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package
minkernel~31bf3856ad364e35~amd64~~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-BootEnvironment-Dvd-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
       Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-Branding-Professional-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim end
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00Co4FC295EE\} \\ Microsoft-Windows-Branding-Professional \\ WMC-Package \\ \sim \\ 31bf3856ad364e35 \\ \sim \\ amd \\ 64 \\ \sim \\ n-1000 \\ \sim \\ n-1000
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-
Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
{\tt 00C04FC295EE} \verb+\Microsoft-Windows-BusinessScanning-Feature-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Package-Packa
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature
Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                                                 C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-
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
    Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
ds-31bf3856ad364e35~amd64~-6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Packagenet~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
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                 C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ Microsoft-Windows-Client-Drivers-Package \\ ^{31bf3856ad364e35} \\ ^{amd64} \\ ^{en-Drivers-Package} \\ ^{31bf3856ad364e35} \\ ^{31bf386ad364e35} \\ ^{31bf386ad364} \\ ^{31bf386ad364e35} \\ ^{31bf386ad364e35} \\ ^{31bf386ad364} \\ ^{31bf
US~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
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-Client-Features-Package-avcore ~31bf3856ad364e35 ~amd 64 ~endows-Client-Features-Package-avcore ~31bf3856ad364e35 ~amd 64 ~endows-Avcore ~31bf3866ad364e35 ~amd 64 ~endows-Avcore ~31bf3866ad364e36 ~amd 64 ~endows-Avcore ~31bf3866ad364e36 ~amd 64 ~endows-Avcore ~31bf3866ad364e36 ~amd 64 ~endows-Avcore ~31bf3866ad366 ~
 US~6.2.9200.16384.cat
                                                                                                 C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~en-
```

```
Opens
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-Client-Features-Package
 base \hbox{$^{+}$31bf3856ad364e35} \hbox{$^{+}$amd64} \hbox{$^{+}$6.2.9200.16384.cat}
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE \} \\ Microsoft-Windows-Client-Features-Package-com \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endormal \\ \sim endormal
 US~6.2.9200.16384.cat
 Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-Client-Features-Package-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11D1-85E5-11
 com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ Microsoft-Windows-Client-Features-Package-drivers-31bf3856ad364e35-amd64-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
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds-31bf3856ad364e35-amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
Opens: C. Wallouws-Systems2/teatroot(1756663-38EE-1101-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds-31bf3856ad364e35-amd64-e-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package-inetcore \\ \sim 31bf3856ad364e35 \\ \sim amd \\ 64 \\ \sim ended \\
 US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Packageinetcore-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mergedcomponents-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mincore-31bf3856ad364e35-amd64-en-
 US~6.2.9200.16384.cat
         Opens:
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package mincore-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-Client-Features-Package-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3856ad364e35-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-en-minio-31bf3866ad364-amd64-amd64-en-minio-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-
 US~6.2.9200.16384.cat
Opens:
                                                                                                                        C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
minio-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODCO4FC295E}\Microsoft-Windows-Client-Features-Package-
multimedia-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\(F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-Client-Features-Package-net~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 US~6.2.9200.16384.cat
 Opens:
 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-
 00C04FC295EE\} \\ \ Microsoft-Windows-Client-Features-Package-terms rv\sim 31bf3856ad364e35\sim amd 64\sim ended for the control of the
  US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
  termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
 00C04FC295EE \} \\ \ Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-defined by the second of the second 
 US~6.2.9200.16384.cat
 Opens: C: \windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\wicrosoft-Windows-Client-Features-Package-100C04FC295EE}
 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-Client-Features-Package-
 00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                        C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
         Opens:
Opens: C. Williams (a) Stemp2 (cathout (1730-00-35) (c. Williams (a) Stemp2 (c. Willia
```

```
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                               C: \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-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
     Opens:
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-COM-MSMQ-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Common-DriverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-Package-base-31bf3856ad364e35-amd64-en-driverClasses-31bf3856ad364e35-amd64-en-driverClasses-31bf3856ad364e35-amd64-en-driverClasses-31bf3856ad364e35-amd64-en-driverClasses-31bf3856ad364e35-amd64-en-driverClasses-31bf3856ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e36-amd64-en-driverClasses-31bf386ad364e36-amd64-en-driverClasses-31bf386ad364e36-amd64-en-driverClasses-31bf386ad364e35-amd64-en-driverClasses-31bf386ad364e36-amd64-en-driverClasses-31bf386ad364e36-amd64-en-driverClasses-31bf386ad364e36-amd64-en-driverClasses-31bf386ad364e36-amd64e366-amd64e36-amd64e36-amd64e36-amd64e36-amd64e36-amd64e36-amd64e36-amd64e36-amd64e36-amd64e36-
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-Common-DriverClasses-Package} \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-brackage \\ \sim amd64 \\ \sim amd
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
OCCO4FC295EE}\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-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~31bf3856ad364e35~amd64~en-drivers-Package-admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admin~admi
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
 admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-ds~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~~6.2.9200.16384.cat
US~6.2.9200.16384.cat
      Opens:
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-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
Opens:
Opens: 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-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat

        US-6.2.9200.16384.Cat
        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-11D1-85E5-0pens:

US~6.2.9200.16384.cat
Opens: C: \verb|Windows| System32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE| \verb|Microsoft-Windows-CoreSystem-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-Package-31bf3856ad364e35-amd64-en-Base-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-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-a
US~6.2.9200.16384.cat
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-
Package~31bf3856ad364e35~amd64~~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-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
     Opens:
                                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
     Opens:
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-CoreSystem-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ \sim ende
US~6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\wicrosoft-\windows-CoreSystem-Package-31bf3856ad364e35-amd64~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \mbox{Microsoft-Windows-CoreSystem-RemoteFS-Base-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-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e35-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad364e36-amd64-en-package-31bf3866ad366-amd64-en-package-31bf3866ad366-amd64666-amd66666-amd66666-amd66666-amd66666-amd666666-amd666666-amd6666666-amd666666-amd6
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
 00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                           C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-Base-Package~31bf3856ad364e35-amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE \} \\ \ Microsoft-Windows-CoreSystem-WOW64-Com-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf386ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf386ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 11bf386ad364e35 \\ \sim amd64 \\ \sim en-Package \\ 
US~6.2.9200.16384.cat
Opens:
                                                                                           C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-CoreSystem-WOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364e35-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3856ad364-amd64-en-MOW64-DS-Package-31bf3866-amd64-amd64-en-MOW64-DS-Package-31bf3866-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-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-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
00C04FC295EE}\Microsoft-Windows-CoreSystem-W0W64-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:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-\%indows-CoreSystem-W0W64-Minio-
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-
 00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-CoreSystem-WOW64-Net-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-Package \\ \sim 10c04FC295EE \\ > 10c04FC
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-Package~31bf3856ad364e35~amd64~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
       Opens
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                           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-DirectoryServices-ADAM-Client-Package
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                          C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                           C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-
```

```
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
 admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE \} \\ Microsoft-Windows-Disk-Diagnosis-Package \\ ^{31bf3856ad364e35} \\ ^{amd64} \\ ^{en-Diagnosis} \\ ^{10c} 
 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\{r750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package-31bf3856ad364e35-amd64-en-
  US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Editions-Professional-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \ Microsoft-Windows-Editions-Professional \\ WMC-Package \sim 31bf3856ad364e35 \sim amd 64 \sim ended \\ \ Corrected by the following of the following states of the fo
 US~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
  00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
        Opens:
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \verb+\Microsoft-Windows-FCI-Client-Package-31bf3856ad364e35-amd64-en-defined by the statement of the statement o
 US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Foundation-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-admin-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-admin-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE\} \\ \mbox{Microsoft-Windows-GroupPolicy-ClientExtensions-Package} \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim endormal \\ \sim endorm
 US~6.2.9200.16384.cat
 Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-GroupPolicy-ClientExtensions-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
        Opens:
 00C04FC295EE\} \\ Microsoft-Windows-GroupPolicy-ClientTools-Package-admin~31bf3856ad364e35~amd64~en-defined by the control of 
 US~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
  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-
 US~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
base-31bf3856ad364e35-amd64~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 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-U5-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package drivers~31bf3856ad364e35~amd64~6.2.9200.16384.cat
                                                                                                              C:\Windows\System32\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-
 OOC04FC295E}\Microsoft-Windows-GroupPolicy-ClientTools-Package-enduser~31bf3856ad364e35~amd64~6.2.9200.16384.cat
                                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 OOC04FC295E}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetcore-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 inetcore~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-inetsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
  inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
  00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio-31bf3856ad364e35-amd64--6.2.9200.16384.cat
 Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\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
 minkernel~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
 Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
 multimedia-31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00Co4FC295EE\} \\ Microsoft-Windows-GroupPolicy-ClientTools-Package-net \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim n-1000 \\ \sim 1000 \\ \sim 1
                                                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
00C04FC295EE\} \land Microsoft-Windows-GroupPolicy-ClientTools-Package-shell \sim 31bf3856ad364e35 \sim amd 64 \sim end of the control of 
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-termsrv-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295E}\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-U5~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODCOMPC295E}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Onens:
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
       Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-
Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-HandwritingRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-
Package-31bf3856ad364e35-amd64--6.2.9200.16384.cat
                                                                                             C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6 2 9200 16384 cat
       Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-Package-31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                                              C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-
Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE\} \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\Microsoft-Windows-IE-Troubleshooters-Package-31bf3856ad364e35-amd64-en-100c04FC295EE] \verb+\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-Window
US~6.2.9200.16384.cat
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \label{lem:cosoft-windows-IIS-WebServer-Add0n-2-Package} \\ 21bf3856ad364e35 \\ \\ 2amd64 \\ \\ 2nmd64 \\ \\ 2
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-IIS-WebServer-AddOn-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
       Opens:
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ImageBasedSetup-IE-Package-Base-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C: \verb|WindowsSystem32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-ImageBasedSetup-IE-Package-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-ImageBasedSetup-III-Windows-ImageBasedSetup-III-Windows-ImageBasedSetup-III-Windows-ImageBasedSetup-III-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-II-Windows-ImageBasedSetup-Image
Base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-enduser-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
      Opens:
                                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-ImageBasedSetup-IE-Package-windows-31bf3856ad364e35-amd64\sim-6.2.9200.16384.cat
Opens: C: \windows \system 32 \catroot \F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \windows-Internet \ensuremath{\system} Explorer-0ptional-Package-31bf3856ad364e35-amd64-ensuremath{\system} Absolute \ensuremath{\system} Explorer-0ptional-Package-31bf3856ad364e35-amd64-ensuremath{\system} Explorer-0ptional-Package-31bf3856ad364e35-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-amd64-
US~10.0.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
                                                                                              C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-InternetExplorer-Package-shell \\ ~31bf3856ad364e35\\ ~amd64\\ ~endered \\ ~amd64\\ ~am
 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
                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~en-
```

```
Opens
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-InternetExplorer-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim ended \\ 
US~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-00C04FC295E}\Microsoft-Windows-InternetExplorer-Package-31bf3856ad364e35-amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Killbits-Package~31bf3856ad364e35-amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Media-Format-Package-avcore~31bf3856ad364e35~am
US~6.2.9200.16384.cat
                                                               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
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-windows-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-Media-Format-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
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-
OOCO4FC295EE}\Microsoft-Windows-Media-Streaming-Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-avcore~31bf3856ad364e35~amd64~en-
US~6 2 9200 16384 cat
    Opens:
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-avcore~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-MediaCenter-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Packageavcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C: \verb|Windows\System32\catroot| F750E6C3-38EE-11D1-85E5-\\
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
base-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                               C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
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-
OOCO4FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
    Opens:
                                                               C:\Windows\Svstem32\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-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
shell \hbox{$^{-}$31bf3856ad364e35$$$^{-}$ amd64$$$^{-}$ 6.2.9200.16384.cat}
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
    Opens:
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
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-MobilePC-Client-Sensors-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
```

```
Opens
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~amd64~en
US~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
   Opens
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{E750E6C3-38EE-11D1-85E5-
  Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Onens:
                                         C:\Windows\System32\catroot\{E750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
ds-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
Opens:
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
enduser~31bf3856ad364e35~amd64~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-inetcore~31bf3856ad364e35~amd64~en-
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
inetcore-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-Multilingual-Package-minkernel-31bf3856ad364e35-amd64-en-defined by the control of the co
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-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~en-
US~6.2.9200.16384.cat
                                         C:\Windows\System32\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-
  Opens:
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
   Opens:
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
windows-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-NetFx-
AutoNgenEnable.3.5~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
ODCO4FC295EE}\Microsoft-Windows-NetFx-
NgenAssemblyExclusionClient-31bf3856ad364e35-amd64~-6.2.9200.16384.cai
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Misc~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-M0F-
Client~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-Extended-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
   Opens:
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                       C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Typelibs~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpNamespace \sim 31bf3856ad364e35 \sim amd64 \sim \sim 6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-MsmqActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
PipeActivation-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
TcpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                         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-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                         C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
```

```
Opens
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-VCRedist-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Windows-Built-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-0C-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-0C-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-0C-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~en
US~6.2.9200.16384.cat
     Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \ Microsoft-Windows-NetFx4-WCF-US-0C-Package \\ \sim 31bf3856ad364e35 \\ \sim amd64 \\ \sim en-1000 \\ \sim 1000 \\ \sim 1
US~6.2.9200.16384.cat
US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-0C-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package-31bf3856ad364e35-amd64-en-
US-6.2.9200.16384.cat
US~6.2.9200.16384.cat
                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \setminus Microsoft-Windows-Parental Controls-Package \sim 31bf3856ad364e35 \sim amd 64 \sim end of the control 
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
      Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-PeerToPeer-Full-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
\label{thm:condition} Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-Personalization-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~en
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00\dot{C}04FC295EE\}\\ \label{lem:consoft-windows-playToManager-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} Opens: C:\\ \label{lem:consoft-windows-playToManager-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} Copens: C:\\ \label{lem:consoft-windows-playToManager-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-play-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-play-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-play-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd64~-6.2.9200.cat} C:\\ \label{lem:consoft-windows-package-31bf3856ad364e35-amd646ad364e364.cat} C:\\ \label{lem:consoft-windows-package-31bf386ad364e364} C:\\ \la
US~6.2.9200.16384.cat
                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-
windows-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-31bf3856ad364e35~amd64-en-US-6.2.9200.16384.cat
Opens: C: \verb|Windows\System32| catroot \ \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ \verb|Microsoft-Windows-Portable-Devices-|
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-
Package-31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Presentation-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
      Opens:
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C: \verb|Windows\System32| catroot \ \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ \verb|Microsoft-Windows-Printer-Drivers-|
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Printing-Foundation-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim end 64 \\ \sim
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
\label{lem:opens: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-
```

```
00C04FC295FE}\Microsoft-Windows-Printing-PremiumTools-Package~31bf3856ad364e35~amd64~en-
     Opens:
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-Package~31bf3856ad364e35~amd64~en-
 US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OOCO4FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Professional\MMCEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-PsuedoTool-HashIDSpy-Package~31bf3856ad364e35~a
US~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
Opens. C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-35E5-

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00\dot{C}04FC295EE\}\\ \label{linear} Microsoft-Windows-RasRip-Package~31bf3856ad364e35-amd64~en-US-6.2.9200.16384.cat Opens: C:\\Windows\\System32\\catroot\\{F750E6C3-38EE-11D1-85E5-}
      Opens:
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                 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\System32\catroot\{F750E6C3-38EE-11D1-85E5
00C04FC295EE\} \\ \ Microsoft-Windows-RemoteAssistance-Package-Client \sim 31bf3856ad364e35 \sim amd 64 \sim en-1000 \\ \ Automatical Microsoft-Windows-RemoteAssistance-Package-Client \sim 31bf3856ad364e35 \\ \ Automatical Microsoft-Windows-RemoteAssistance-Package-Client \sim 31bf3856ad364e35 \\ \ Automatical Microsoft-Windows-RemoteAssistance-Package-Client \\ \ Automatical Microsoft-Windows-RemoteAssistance-Package-Windows-Windows-Windows-Windows-Windows-Windows-Windows-Win
US~6.2.9200.16384.cat
Opens: C: \verb|Windows| System 32| catroot| \{F750E6C3-38EE-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-Remote Assistance-Package-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-Remote Assistance-Package-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-Remote Assistance-Package-11D1-85E5-00C04FC295EE\} \\ | Microsoft-Windows-Remote Assistance-Package-11D1-85E5-00C04FC295EE] \\ | Microsoft-Window
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
                                                                                               C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RotMgr-Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C: \windows\system 32\catroot\space{2.5cm} Coco4FC295EE\}\windows-RotMgr-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat and a superior of the control of the co
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
                                                                                                 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\Svstem32\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 \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim end 64 \\ \sim
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-SecureStartup-Package-31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
\label{thm:continuous} Opens: C:\windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf386ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf386ad364e35-amd64~-6.2.9200.16384.catroot\-SecureStartup-Package-31bf386ad364e35-amd64~-6.2.9200.06384.catroot\-SecureStartup-Package-31bf386ad364e35-amd64~-6.2.9200.06384.catroot\-SecureStartup-Package-31bf386ad364e35-amd646ad364.catroot\-SecureStartup-Package-31bf386ad364-amd646ad364.catroot\-SecureS
Opens: C:\Windows\System3\\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-APPXL0B-Client-
 Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
C. WHITHOUS SYSTEMS ZYCETTOOTY (F/SUEBL3-3 00C04FC295EE) Wicrosoft-Windows-Security-SPP-Component-SKU-OCUR-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE)\Microsoft-Windows-Security-SPP-Component-SKU-Professional-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ServicingBaseline-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
Opens:
                                                                                                 C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-Shell-HomeGroup-Package-printscan \sim 31bf3856ad364e35 \sim amd 64 \sim end of the control of the 
 US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
                                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295FE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~en-
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-Wallpaper-Common-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~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-SKU-Foundation-Package-base-31bf3856ad364e35-amd64-endows-skulled 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-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-SKU-Foundation-Package-com-31bf3856ad364e35-amd64-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000-en-2000
                                                                                                    C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C: \windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\wicrosoft-Windows-SKU-Foundation-Package-100C04FC295EE} \windows-SKU-Foundation-Package-100C04FC295EE \windows-SKU-Foundation-Pac
ds-31bf3856ad364e35-amd64-~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\f750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
enduser-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\f750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mergedcomponents-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
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
mincore-31bf3856ad364e35-amd64~-6.2.9200.16384.cat Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE \} \\ \ Microsoft-Windows-SKU-Foundation-Package-minio-31bf3856ad364e35-amd64-end-formula for the control of the 
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-ended and the state of the s
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
 00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                     C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ \label{lem: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
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
       Opens:
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sdktools~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package
```

```
sdktools~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-shell~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
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE\} \land Microsoft-Windows-SKU-Foundation-Package-sql \sim 31bf3856ad364e35 \sim amd 64 \sim end of the contraction of the cont
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
sql~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-SKU-Foundation-Package-ua-31bf3856ad364e35-amount of the control of the
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
     Opens
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~en
US~6.2.9200.16384.cat
     Opens
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SpeechRecognizer-Package~31bf3856ad364e35~amd64
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                            C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                            C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~er
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Store-Client-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens:
                                                                            C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \\ Microsoft-Windows-TabletPC-Package \\ \sim 31bf3856ad364e35 \\ \sim amd 64 \\ \sim en-US \\ \sim 6.2.9200.16384.cat
                                                                            C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C: \windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-Telnet-Client-Package-31bf3856ad364e35-amd64-ender Client-Package-31bf3856ad364e35-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf3856ad364-amd64-ender Client-Package-31bf386ad364-amd64-ender Client-Pa
US~6.2.9200.16384.cat
     Opens:
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
\label{thm:condition} Opens: C:\windows\system32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-Telnet-Server-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.catroot\arrowvertex.
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
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: \verb|Windows| System32| catroot| F750E6C3-38EE-11D1-85E5-00C04FC295EE} \\ | Microsoft-Windows-Terminal Services-WMIProvider- | Microsoft-WMIProvider- | Microsoft-WMIProv- | Microsoft-WMIProvider- | Microsoft-WMIProvider- | Microsoft
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                            C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
```

```
Opens
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat 
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WebcamExperience-Package-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
 00C04FC295EE}\Microsoft-Windows-WebcamExperience
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \land Microsoft-Windows-WindowsFoundation-LanguagePack-Package \sim 31bf3856ad364e35 \sim amd 64 \sim en-1000 \times 1000 \times
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
 00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore-31bf3856ad364e35-amd64-en-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore-31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00Co4FC295EE\} \\ Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.categorians and the contraction of the contraction 
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Win0cr-Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
OCCO4FC295EE}\Microsoft-Windows-WinSATMediaFiles-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE\} \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-WMI-SNMP-Provider-Package-31bf3856ad364e35-amd64-en-100C04FC295EE] \verb+\Microsoft-Windows-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SNMP-WMI-SN
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-WMPNetworkSharingService-Package avcore-31bf3856ad364e35-amd64-en-US-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPMetworkSharringService-Package-
avcore-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\\F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-\mPNetworkSharingService-
Package-31bf3856ad364e35-amd64~-6.2.9200.16384.cat
                                                                                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens:
O0C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-
Package~31bf3856ad364e35-amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-
Package-31bf3856ad364e35-amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\nt5.cat
                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
      Opens
00C04FC295EE}\ntexe.cat
                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
     Opens:
00C04FC295EE}\ntpe.cat
      Opens
                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\ntph.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\oem0.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}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Server-Help-Package.ClientProfessional=31bf3856ad364e35~amd64~~6.2.9200.16384.cat
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
                                                                                  C:\Windows\Svstem32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-Group-Policy-Package-31bf3856ad364e35-and64~-6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
 00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
                                                                                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\windows-legacy-whql.cat
      Opens:
                                                                                  C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
      Opens:
                                                                                  C:\Windows\Branding
C:\Windows\Branding\Basebrd
      Opens:
      Opens:
                                                                                  C:\Windows\System32\en-US
C:\Windows\System32\KernelBase.dll
      Opens:
      Opens:
       Opens:
                                                                                   C:\Windows\System32\locale.nls
                                                                                  C:\Windows\System32\advapi32.dll
      Opens:
                                                                                   C:\Windows\System32\msvcrt.dll
       Opens:
                                                                                  C:\Windows\System32\rpcrt4.dll
C:\Windows\System32\ole32.dll
      Opens:
       Opens:
      Opens:
                                                                                  C:\Windows\System32\oleaut32.dll
                                                                                  C:\Windows\System32\combase.dll
       Opens:
       Opens:
                                                                                  C:\Windows\System32\gdi32.dll
       Opens
                                                                                  C:\Windows\System32\en-US\sppsvc.exe.mui
```

```
C:\Windows\System32\rpcss.dll
     Opens
                                                                                    \Windows\System32\cryptbase.dll
      Opens:
     Opens:
                                                                             C:\Windows\System32\bcryptprimitives.dll
C:\Windows\System32\sppobjs.dll
                                                                             C:\Windows\Branding\Basebrd\basebrd.dll
C:\Windows\System32\wwapi.dll
     Opens:
     Opens:
                                                                             C:\Windows\System32\\spp\\store\data.dat
C:\Windows\System32\\spp\plugin-manifests-signed\\sppwinob-spp-plugin-
     Opens:
manifest-signed.xrm-ms
     Opens:
                                                                             C:\Windows\System32\sppwinob.dll
                                                                             C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll
     Opens:
     Opens:
                                                                             C:\Windows\System32\srvcli.dll
C:\Windows\System32\wkscli.dll
     Opens:
     Opens:
                                                                             C:\Windows\System32\dsrole.dll
                                                                             {\tt C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-signed\sppobjs-spp-plugin-manifests-spp-plugin-manifests-spp-plugin-manifests-spp-plugin-manifests-spp-plugin-manifests-spp-plug
     Opens:
manifest-signed.xrm-ms
                                                                             C:\Windows\System32\spp\store\cache\cache.dat
     Opens:
     Opens:
                                                                                    \Windows\System32\spp\store\tokens.dat
     Opens:
                                                                             C:\Windows\System32\spp\store\data.dat.tmp
C:\Windows\System32\spp\store
                                                                            C:\Windows\System32\spp\store\data.dat.bak
C:\Windows\System32\clbcatq.dll
     Opens:
     Opens:
     Opens:
Opens:
                                                                             C:\Windows\Svstem32\en-US\KernelBase.dll.mui
                                                                             C:\Windows\System32\bcrypt.dll
                                                                            C:\Windows\System32\taskschd.dll
C:\Windows\System32\sspicli.dll
     Opens:
     Opens:
                                                                             C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
     Writes to:
     Writes to:
     Writes to
                                                                             C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\@
Writes to: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
Writes to:
1001\$I5D1DD46B
                                                                             C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
                                                                             C:\Windows\assembly\GAC_64\Desktop.ini
C:\Windows\assembly\GAC_32\Desktop.ini
C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
     Writes to:
     Writes to:
     Writes to:
                                                                             C:\Windows\System32\spp\store\data.dat.tmp
C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
    Writes to:
     Reads from:
                                                                             C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
     Reads from:
     Reads from:
                                                                             C:\Users\desktop.ini
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
     Reads from:
     Reads from:
     Reads from:
                                                                             C:\Users\Admin\Desktop\desktop.ini
C:\Users\Public\desktop.ini
     Reads from:
     Reads from:
                                                                             C:\Users\Public\Desktop\desktop.ini
     Reads from:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
Readsfrom: C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
     Reads from:
                                                                             C:\Windows\System32\spp\store\data.dat
                                                                             \hbox{\tt 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-signed\sppwinob-spp-plugin-manifests-s
     Reads from:
manifest-signed.xrm-ms
                                                                             C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
   Reads from:
manifest-signed.xrm-ms
     Reads from:
                                                                             C:\Windows\System32\spp\store\cache\cache.dat
                                                                             C:\Windows\System32\spp\store\tokens.dat
     Reads from:
     Deletes:
                                                                             C:\Windows\Temp\26ec828da6d2651f90c74cb275b800cc.exe
     Deletes:
                                                                             C:\Windows\System32\spp\store\data.dat.tmp
```

Network Events

DNS query:	
	j.maxmind.com
	j.maxmind.com ⇒ 127.0.0.1
	127.0.0.1:80
	8.8.8.53
	83.133.123.20:53
	206.254.253.254:16470
	197.254.253.254:16470
	190.254.253.254:16470
	184.254.253.254:16470
	183.254.253.254:16470
	182.254.253.254:16470
	180.254.253.254:16470
	166.254.253.254:16470
	158.254.253.254:16470
	135.254.253.254:16470
	134.254.253.254:16470
	119.254.253.254:16470
	117.254.253.254:16470
	115.254.253.254:16470
	113.254.253.254:16470
	69.121.230.254:16470
	1.186.134.249:16470
	193.30.251.248:16470
	2.192.37.245:16470
	117.109.27.245:16470
	49.205.25.244:16470
	75.65.128.242:16470
	71.206.79.242:16470
	76.94.226.239:16470
	66.66.109.239:16470
	98.143.7.239:16470
	188.25.115.238:16470
	69.141.58.238:16470
	137.186.139.237:16470
	174.4.174.236:16470
	24.21.90.235:16470
	78.84.103.234:16470
	74.115.1.233:16470
	24.144.182.232:16470
	88.68.214.231:16470
	87.72.8.231:16470
	82.235.17.230:16470
	69.31.207.228:16470
	58.192.124.226:16470
	70.180.117.226:16470
	173.175.60.222:16470
	68.96.219.221:16470
Sends data to:	78.82.44.221:16470

```
Sends data to:
                                   76.173.167.219:16470
                                  24.129.52.219:16470
87.144.119.218:16470
Sends data to:
Sends data to
                                  109.235.54.216:16470
69.119.40.216:16470
Sends data to:
Sends data to:
Sends data to:
Sends data to:
                                  24.90.159.214:16470
75.64.60.214:16470
Sends data to
                                   96.25.185.213:16470
                                   98.223.195.212:16470
Sends data to:
Sends data to:
                                  178.5.229.211:16470
37.3.34.210:16470
Sends data to:
```

Receives data from 0.0.0.0:0 Windows Registry Events Creates key: HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication HKU\s-1-5-18\software\classes\clsid Creates key: Creates key HKU\.default\software\classes\clsid Creates key HKU\.default\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e93 HKU\.default\software\classes\clsid\{fbeb8a05-beee-4442-804e-Creates key: 409d6c4515e9}\inprocser er32 HKCU\software\microsoft\internet explorer\toolbar Creates key: Creates key HKCU\software\microsoft\internet explorer\toolbar\shellbrowser Creates key HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\ Creates key HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity Creates key $\label{thm:local} HKLM \system \current controls et \control \graphics drivers \configuration \control \graphics drivers \configuration \configuration \graphics \graphic \g$ Creates key: Creates key: Creates key HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106 Creates key: center\checks\{e8433b72-HKCU\software\microsoft\windows\currentversion\action 5842-4d43-8645-bc2c35960837}.check.101 $\label{local-cross-continuous} Creates key: \\ HKCU\software\microsoft\windows\currentversion\action center\checks\eastable 2-4443-8645-bc2c35960837\}.check.103$ Creates key $\label{local-cross-continuous} Creates key: \\ HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.100$ Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102 HKCU\software\microsoft\windows\currentversion\action Creates key: center\checks\{e8433b72-5842-4d43-8645-bc2c35960837},check.104 Creates key: HKCU\software\microsoft\windows\currentver center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\.check.100 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\currentversion\action center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0 $\label{lem:creates} Creates key: $$ HKCU\software\microsoft\windows\currentversion\action center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0$$ Creates key: Creates key: $\label{thm:local-prop} $$HKCU\software\microsoft\windows\currentversion\startupnotify $$HKCU\software\microsoft\windows\currentversion\action $$$ center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0 HKCU\software\microsoft\windows\currentversion\action Creates key: center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018} HKCU\software\microsoft\windows\currentversion\action Creates key center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100 HKCU\software\microsoft\windows\currentversion\action Creates key: center\checks\{01979c6a 42fa-414c-b8aa-eee2c8202018}.check.101 HKCU\software\microsoft\windows\currentversion\action Creates key center\provid entlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881} Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\ 4d2a-4d44-94bf-e0091898c881}.check.100 Creates key HKCU\software\microsoft\windows\currentversion\action ventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78} center\providers\e Creates key: center\checks\{11cd958a HKCU\software\microsoft\windows\currentversion\action-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101 $\label{local-continuous} Creates key: \\ HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a\}}$ Creates key: $\label{local-continuous} Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a\}.check.100$ Creates key: HKCU\software\microsoft\windows\current\center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}.check.800 Creates key: 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 Creates key: HKCU\software\microsoft\windows\current\ center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b} HKCU\software\microsoft\windows\currenty Creates key: center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100 HKCU\software\microsoft\windows\currentversion\action Creates key: center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100 Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482\}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action ventlog\{2374911b-b114-42fe-900d-54f95fee92e5} center\provider HKCU\software\microsoft\windows\currentversion\action 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 Creates key: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc} HKCU\software\microsoft\windows\currentversion\action Creates key: center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100 Creates key: HKLM\system\wpa Creates key: HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34 Deletes value HKLM\software\microsoft\windows\currentversion\run[windows defender]

Opens key: HKI M\softwa e\wow6432node\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: Opens key

Opens key: Opens key

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers HKLM\system\currentcontrolset\control\nls\customlocale Opens key

HKLM\system\currentcontrolset\control\terminal server HKLM\system\currentcontrolset\control\safeboot\option

HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key HKLM\system\currentcontrolset\control\nls\language

HKLM\software\microsoft\wow64

```
Opens key:
                              HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:
                              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
                              \label{thm:local-policies} HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key
  Opens key:
  Opens key
                              HKLM\software\policies\microsoft\mui\settings
  Opens key
                              HKCU\
                              \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
                              HKCU\control panel\desktop\languageconfiguration
  Opens key
                              HKCU\control panel\desktop
HKCU\control panel\desktop\muicached
  Opens key
  Opens key
  Opens key:
                              HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
                              HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:
  Opens key:
                              \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ \arrowversion \approximately a gradual constraint $$ \arrowversion \ar
                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key
  Opens key:
                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:
                              HKLM\system\currentcontrolset\control\session manager
  Opens key:
                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
 Opens key
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key
                              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key: HKLM\sof
nt\currentversion\compatibility32
                              HKLM\software\wow6432node\microsoft\windows
  Opens key
                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:
                              HKI M\
                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:
                              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
  Opens key:
                              HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\wow6432node\microsoft\direct3d
  Opens key:
  Opens kev:
                              HKLM\software\policies\microsoft\samclient\windows
                              HKLM\software\microsoft\sqmclient\windows
  Opens key:
  Opens kev:
                              HKLM\system\currentcontrolset\services\crypt32
                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
  Opens key:
  Opens key
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\26ec828da6d2651f90c74cb275b800cc.exe
  Opens key:
                              {\tt HKLM \ } system \verb|\ current controlset \verb|\ control \ session \ manager \verb|\ appcertdlls| \\
                              HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:
  Opens key
                              HKLM\software\wow6432node\policies\microsoft\windows\appcompat
  Opens key
  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
                              HKLM\software\wow6432node\microsoft\windows
  Opens key:
nt\currentversion\appcompatflags\custom\26ec828da6d2651f90c74cb275b800cc.exe
                              HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:
  Opens kev:
                              \label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows}\ nt\current\version\app\compatflags\layers}
  Opens key:
                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\26ec828da6d2651f90c74cb275b800cc.exe
 Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:
                              {\tt HKLM \backslash system \backslash current controlset \backslash control \backslash compression}
                              HKLM\system\currentcontrolset\services\winsock2\parameters
HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:
  Opens key:
  Opens key:
                              \label{lem:hklmsystem} \\ \textbf{HKLM} \\ \textbf{system} \\ \textbf{current control set \ control \ nls \ sorting \ ids} \\
                              HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog
  Opens key:
  Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog\136a17c6
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalogs
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\00000005
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
  Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
Opens kev:
Opens kev:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000000001
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000000
  Opens key:
Opens key:
Opens key:
```

HKLM\system\currentcontrolset\services\winsock\parameters

Opens key:

```
Opens key:
                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
    Opens key:
                                                      \label{lem:hklm} \verb+KLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens key
                                                     HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
   Opens key:
HKLM \label{lem:hklm} \verb| hklm| software \verb| wow6432 node \verb| microsoft| cryptography \verb| defaults \verb| provider \verb| microsoft| base cryptographic | microsoft| cryptographic | microsoft| cryptography | mic
provider v1.0
Opens key:
                                                     HKLM\software\policies\microsoft\cryptography
   Opens key:
                                                     HKLM\software\microsoft\cryptography
HKLM\software\wow6432node\microsoft\cryptography\offload
   Opens key:
   Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
                                                     HKLM\software\microsoft\windows nt\currentversion\windows
   Opens key:
   Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus root \setminus certificates \setminus 2bd63d28d7bcd0e251195aeb519243c13142ebc3
   Opens key:
Opens key:
HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
   Opens key:
                                                     HKLM\system\currentcontrolset\services\windefend
                                                     HKLM\system\currentcontrolset\services\windefend\security
    Opens kev:
   Opens kev:
                                                     HKLM\system\currentcontrolset\services\windefend\triggerinfo
   Opens key:
                                                     Opens key:
952f-41f1-9a6f-135d9c6622cc}
   Opens key:
aa9d-4618-a949-c1b91af43b1a}
                                                     HKLM\software\microsoft\windows\currentversion\run
HKLM\software\wow6432node\microsoft\rpc
   Opens key:
   Opens key:
                                                      HKLM\system\currentcontrolset\control\computername\activecomputername
    Opens key
   Opens key:
                                                     HKLM\system\setup
    Opens key:
                                                      Opens key
                                                     HKLM\software\policies\microsoft\windows nt\rpc
    Opens key:
                                                      HKLM\system\currentcontrolset\control\sqmservicelist
   Opens kev:
                                                     HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
    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:
Opens key:
Opens kev:
Opens kev:
Opens kev:
Onens key
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\00000000000005
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\00000000000003
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\00000000000001
                                                     HKLM \label{lem:hklm} \begin{tabular}{ll} HKLM \label{lem:hklm} software \mbox{$\mathbb{N}$ icrosoft base} \\ \end{tabular}
   Opens key:
cryptographic provider v1.0
   Opens key:
                                                     HKLM\software\microsoft\cryptography\offload
                                                     \label{thm:hammon} HKLM \software \microsoft \cryptography \deshashs ession keybackward \ HKLM \software \microsoft \windows nt \current version \profile list \ \cryptography \cryptography \deshashs ession \cryptography \deshashs \cryptogr
   Opens key:
   Opens key:
   Opens key:
                                                     {\tt HKLM \ } system \verb| current control \verb| session manager \verb| environment| \\
                                                     HKLM\software\microsoft\windows\currentversion
   Opens key:
   Opens key:
                                                     HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
                                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Opens key:
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
                                                     HKU\.default\environment
   Opens key:
   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:
                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe\perfoptions
                                                     HKU\.default\software\microsoft\windows
   Opens key:
nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
\verb|nt\currentversion\appcompatflags\custom\rundl132.exe|
   Opens key:
                                                     HKLM\software\microsoft\windows\currentversion\sidebyside
   Opens key:
Opens key:
                                                     \label{lem:hkuldefaultsoftware policies microsoft windows safer code identifiers $$HKU\.default\control$$
\label{thm:local_ham} $$HKU\.default\control\ panel\desktop\label{thm:hku} Iku\.default\control\ panel\desktop $$
   Opens key:
   Opens key
   Opens key:
                                                     HKU\.default\control panel\desktop\muicached
                                                     HKLM\system\currentcontrolset\control\error message instrument\
   Opens kev:
    Opens key:
                                                      HKLM\system\currentcontrolset\control\error message instrument
   Opens key
                                                     HKLM\software\microsoft\windows nt\currentversion\gre initialize
                                                      HKLM\software\microsoft\windows nt\currentversion\compatibility32
    Opens key:
   Opens kev:
                                                     HKLM\software\microsoft\windows nt\currentversion\ime compatibility
                                                      HKLM\system\currentcontrolset\control\cmf\config
   Opens key:
   Opens key
                                                     HKLM\software\microsoft\rpc
                                                     HKLM\system\currentcontrolset\services\bfe
    Opens key:
```

HKLM\system\currentcontrolset\services\bfe\startoverride

HKLM\system\currentcontrolset\services\aelookupsvc

Opens key

Opens key

```
Opens key
                                                                 HKLM\system\currentcontrolset\services\aelookupsyc\triggerinfo
                                                                  HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
     Opens key:
                                                                 \label{thm:hklm-system-current} HKLM\system\currentcontrolset\services\alg
     Opens key
     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
    Opens key
     Opens key
                                                                 HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
                                                                 HKLM\system\currentcontrolset\services\appinfo
    Opens key
     Opens key
                                                                  HKLM\system\currentcontrolset\services\appinfo\triggerinfo
    Opens key
                                                                 HKLM\system\currentcontrolset\services\appmgmt
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
     Opens key
                                                                 HKLM\system\currentcontrolset\services\audioendpointbuilder
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
    Opens key
                                                                 HKLM\system\currentcontrolset\services\audiosrv
                                                                  HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
     Opens key:
     Opens key
                                                                 HKLM\svstem\currentcontrolset\services\axinstsv
                                                                  HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
     Opens key:
    Opens key
                                                                 HKLM\svstem\currentcontrolset\services\bdesvc
    Opens key:
                                                                  HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
    Opens key:
Opens key:
                                                                 HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0 HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
                                                                 HKLM\system\currentcontrolset\services\bfe\triggerinfo
    Opens key
    Opens key
     Opens key
                                                                 HKLM\system\currentcontrolset\services\bits\triggerinfo
                                                                 HKLM\system\currentcontrolset\services\brokerinfrastructure
    Opens key
                                                                  HKLM \setminus system \setminus current control set \setminus services \setminus broker in frastructure \setminus trigger in formula in the system in the system of the system in the system of th
     Opens key:
     Opens key
                                                                 HKLM\system\currentcontrolset\services\browser
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\browser\triggerinfo
    Opens key
                                                                 HKLM\system\currentcontrolset\services\browser\triggerinfo\0
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\browser\triggerinfo\1
     Opens key
                                                                 HKLM\system\currentcontrolset\services\browser\triggerinfo\2
                                                                  HKLM\system\currentcontrolset\services\browser\startoverride
     Opens key
    Opens key
                                                                 HKLM\svstem\currentcontrolset\services\bthserv
     Opens key:
                                                                  {\tt HKLM \ system \ current control set \ services \ bthserv \ trigger info}
     Opens key
                                                                 HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
    Opens key:
                                                                 HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
                                                                 HKLM\system\currentcontrolset\services\certpropsvc
HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
    Opens key
    Opens key
     Opens key
                                                                 HKLM\system\currentcontrolset\services\comsysapp
HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
    Opens key
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\cryptsvc
                                                                 HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo HKLM\system\currentcontrolset\services\cscservice
     Opens key
     Opens key
                                                                 HKLM\system\currentcontrolset\services\cscservice\triggerinfo
    Opens key
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0
     Opens key
                                                                 HKLM\svstem\currentcontrolset\services\cscservice\triggerinfo\1
                                                                  HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
     Opens key
    Opens key
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \microsoft \telemetry client \throttlestore \sqm\windows \winsqm8 \end{tabular}
    Opens key:
                                                                 \label{thm:hklm-soft-with-soft-soft-lemetryclient-throttlest-ore-sqm-windows HKLM-soft-ware-microsoft-telemetryclient-throttlest-ore-sqm-windows through the soft-ware-windows and the soft-ware-windows through the s
     Opens key:
    Opens key
                                                                 HKLM \software \mbox{$\stackrel{\cdot}{\rm MKLM} \software \mbox{$\stackrel{\cdot}{\rm MKLM}
    Opens key
                                                                 HKLM\software\microsoft\telemetryclient\samplestore\sqm\windowsHKLM\software\microsoft\telemetryclient\samplestore\sqm
     Opens key
    Opens key
     Opens key
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
HKLM\software\microsoft\telemetryclient\throttlestore\sgm\windows\winsgm8\13238784
    Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sgm\windows\winsam8\13238784
                                                                  HKLM\system\currentcontrolset\services\dcomlaunch
     Opens key:
                                                                 HKLM\svstem\currentcontrolset\services\dcomlaunch\triggerinfo
     Opens kev:
                                                                  HKLM\system\currentcontrolset\services\defragsvc
     Opens key:
    Opens key
                                                                 HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
     Opens key:
                                                                 HKLM\system\currentcontrolset\services\deviceassociationservice
    Opens key
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} \textbf{KLM} \end{tabular} set $$ \end{tabular} is a constant of the local property of the loc
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\2
                                                                 HKLM\system\currentcontrolset\services\deviceinstall
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo
    Opens key:
    Opens key
     Opens key:
                                                                  Opens key
                                                                 HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1
     Opens key:
                                                                  HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\2
    Opens key
                                                                 HKLM\svstem\currentcontrolset\services\dhcp
                                                                  HKLM\system\currentcontrolset\services\dhcp\triggerinfo
     Opens key:
     Opens key
                                                                 HKLM\system\currentcontrolset\services\dnscache
    Opens key:
                                                                  HKLM\system\currentcontrolset\services\dnscache\triggerinfo
    Opens key:
Opens key:
                                                                 HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0 HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
    Opens key
                                                                 HKLM\system\currentcontrolset\services\dnscache\startoverrideHKLM\system\currentcontrolset\services\dot3svc
                                                                 Opens key
     Opens key
                                                                 \label{thm:hklmsystem} HKLM \ system \ current controls et\ services \ dps \ trigger info HKLM \ system \ current controls et\ services \ ds m \ svc
    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
    Opens key
                                                                 HKLM\system\currentcontrolset\services\eaphost
                                                                  HKLM\system\currentcontrolset\services\eaphost\triggerinfo
     Opens key:
     Opens key
                                                                 HKLM\system\currentcontrolset\services\efs
                                                                  HKLM\system\currentcontrolset\services\efs\triggerinfo
     Opens key:
    Opens key
                                                                 HKLM\system\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
                                           HKLM\system\currentcontrolset\services\eventsystem
Opens key:
                                           HKLM\system\currentcontrolset\services\fax
HKLM\system\currentcontrolset\services\fax\triggerinfo
Opens key
Opens key
Opens key
                                           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
Opens key
                                           HKLM\system\currentcontrolset\services\fhsvc
HKLM\system\currentcontrolset\services\fhsvc\triggerinfo
Opens key
                                           HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1
Opens key
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\2
                                           HKLM\system\currentcontrolset\services\fontcache
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\fontcache3.0.0.0
Opens key
Opens key:
                                           Opens key
                                           HKLM\system\currentcontrolset\services\gpsvc
Opens key
                                           HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
Opens key
                                           HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\1
Opens key:
Opens key
                                           HKLM\svstem\currentcontrolset\services\hidserv
                                           HKLM\system\currentcontrolset\services\hidserv\triggerinfo
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
Opens key:
                                           HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1
Opens key
                                           HKLM\system\currentcontrolset\services\hkmsvc
HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
                                           HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
Opens key
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\homegroupprovider
                                           HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo
Opens key
                                           Opens key
                                           HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\1
Opens key
                                           HKLM\system\currentcontrolset\services\ikeext
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\svstem\currentcontrolset\services\ivmservice
Opens key:
                                           HKLM\system\currentcontrolset\services\keyiso
                                           \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\keyiso\triggerinfo-00. The local ham are also considered as the local ham are also considered 
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\keyiso\triggerinfo\1 HKLM\system\currentcontrolset\services\ktmrm
Opens key
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\ktmrm\triggerinfo HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
Opens key
                                           HKLM\system\currentcontrolset\services\lanmanserver
Opens key
                                           HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo
Opens key
                                           HKLM\system\currentcontrolset\services\lanmanworkstation
Opens key:
                                           HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo
Opens key
                                           HKLM\svstem\currentcontrolset\services\lmhosts
Opens key:
                                           HKLM\system\currentcontrolset\services\lmhosts\triggerinfo
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
Opens key:
                                           HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\3
                                           HKLM\system\currentcontrolset\services\lsm
HKLM\system\currentcontrolset\services\lsm\triggerinfo
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\mmcss
HKLM\system\currentcontrolset\services\mmcss\triggerinfo
Opens key
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\msdtc
                                           HKLM\system\currentcontrolset\services\msdtc\triggerinfo
Opens key
                                           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
                                           HKLM\system\currentcontrolset\services\ncasvc
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\ncasvc\triggerinfo
Opens key:
                                           HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0
Opens key
                                           HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1 HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2
                                           HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\3 HKLM\system\currentcontrolset\services\ncdautosetup
Opens key
Opens key
Opens key
                                           \label{thm:local_ham} HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\ HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0
                                           \label{thm:hklmsystem} HKLM \system \correct services \ncd autoset up \trigger in fold HKLM \system \current control set \services \net \logon
Opens key
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\netlogon\triggerinfo
Opens key
                                           {\tt HKLM \colored \c
Opens key:
Opens key
                                           HKLM\svstem\currentcontrolset\services\netprofm
Opens key
                                           HKLM\system\currentcontrolset\services\netprofm\triggerinfo
Opens key
                                           HKLM\system\currentcontrolset\services\nettcpportsharing
                                           {\tt HKLM \ } system \ \verb|\ current control set \ \verb|\ services \ \verb|\ nettcpportsharing \ \verb|\ triggerinfo| \\
Opens key:
Opens key
                                           HKLM\system\currentcontrolset\services\nlasvo
Opens key:
                                           HKLM\system\currentcontrolset\services\nlasvc\triggerinfo
Opens key:
Opens key:
                                           HKLM\system\currentcontrolset\services\nsi
                                           HKLM\system\currentcontrolset\services\nsi\triggerinfo
Opens key
                                           HKLM\system\currentcontrolset\services\ose
HKLM\system\currentcontrolset\services\ose\triggerinfo
                                           HKLM\system\currentcontrolset\services\p2pimsvc
HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
Opens key
Opens key
Opens key:
Opens key:
                                           HKLM\system\currentcontrolset\services\p2psvc
HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
                                           HKLM\system\currentcontrolset\services\pcasvc
HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
Opens key:
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\peerdistsvo
Opens key
                                           HKLM\system\currentcontrolset\services\peerdistsyc\triggerinfo
                                           HKLM\system\currentcontrolset\services\perfhost
Opens key:
Opens key
                                           HKLM\system\currentcontrolset\services\perfhost\triggerinfo
                                           HKLM\system\currentcontrolset\services\pla
Opens key:
Opens key
                                           HKLM\system\currentcontrolset\services\pla\triggerinfo
Opens key:
                                           HKLM\system\currentcontrolset\services\plugplay
                                           HKLM\system\currentcontrolset\services\plugplay\triggerinfo
Opens key
Opens key
                                           HKLM\system\currentcontrolset\services\pnrpautoreg
```

```
HKLM\svstem\currentcontrolset\services\pnrpautoreg\triggerinfo
Opens key
Opens key:
                                            HKLM\system\currentcontrolset\services\pnrpsvc
                                            \label{thm:local_ham} HKLM \ system \ current control set \ services \ purps v c \ trigger in fo \ HKLM \ system \ current control set \ services \ policy agent
Opens key
Opens key
Opens key
                                            \label{thm:local_ham} HKLM \system \current controlset \services \policy agent \trigger in fo-00 \end{tikzpicture} \\ HKLM \system \current controlset \services \policy agent \trigger in fo-00 \end{tikzpicture} 
Opens key
Opens key
Opens key
                                            \label{thm:local_hammon} HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1 \\ HKLM\system\currentcontrolset\services\policyagent\startoverride
Opens key
                                            HKLM\system\currentcontrolset\services\power
HKLM\system\currentcontrolset\services\power\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\printnotify
HKLM\system\currentcontrolset\services\printnotify\triggerinfo
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\profsvc
                                            HKLM\system\currentcontrolset\services\profsvc\triggerinfo
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\qwave
                                            HKLM\system\currentcontrolset\services\qwave\triggerinfo
Opens key
Opens key:
                                            HKLM\system\currentcontrolset\services\rasauto
Opens key
                                            HKLM\system\currentcontrolset\services\rasauto\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\rasman
Opens key
                                            \label{thm:basis} $$HKLM\system\currentcontrolset\services\ramn\triggerinfo $$HKLM\system\currentcontrolset\services\ramn\triggerinfo $$HKLM\system\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\
Opens key:
                                            HKLM\svstem\currentcontrolset\services\remoteaccess\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\remoteregistry
Opens key
Opens key
                                            {\tt HKLM \ } system \verb|\ current controlset \verb|\ services \verb|\ remoteregistry \verb|\ triggerinfo
Opens key:
                                            HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0
Opens key:
Opens key:
                                            HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\1 HKLM\system\currentcontrolset\services\rpceptmapper
                                            HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
                                            HKLM\system\currentcontrolset\services\rpcss
Opens key
                                            HKLM\system\currentcontrolset\services\rpcss\triggerinfo
Opens key:
Opens key
                                            HKLM\system\currentcontrolset\services\samss
Opens key:
                                            HKLM\system\currentcontrolset\services\samss\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\scardsyr
Opens key:
                                            HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0
                                            HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\2
Opens key:
                                            Opens key
                                            HKLM\system\currentcontrolset\services\schedule\triggerinfo
Opens key:
                                            HKLM\system\currentcontrolset\services\scpolicysvc
                                            HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo HKLM\system\currentcontrolset\services\sdrsvc
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo HKLM\system\currentcontrolset\services\seclogon
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\seclogon\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\sens
Opens key
                                            HKLM\system\currentcontrolset\services\sens\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\sensrsvc
Opens key:
                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
Opens key
                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2
Opens key:
                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\3
Opens key
                                            HKLM\system\currentcontrolset\services\sessionenv
Opens key:
                                            HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
Opens key
                                            HKLM\svstem\currentcontrolset\services\shellhwdetection
                                            HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\smptrap
HKLM\system\currentcontrolset\services\smptrap\triggerinfo
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\spooler
HKLM\system\currentcontrolset\services\spooler\triggerinfo
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\sppsvc
                                            HKLM\system\currentcontrolset\services\sppsvc\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\1
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\ssdpsrv
                                            HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\sstpsvc
Opens key:
Opens key
                                            HKLM\svstem\currentcontrolset\services\sstpsvc\triggerinfo
                                            HKLM\system\currentcontrolset\services\stisvc
Opens key
Opens key
                                            HKLM\svstem\currentcontrolset\services\stisvc\triggerinfo
Opens key:
                                            HKLM\system\currentcontrolset\services\storsvc
Opens key:
Opens key:
                                            \label{thm:local} $$HKLM\system\currentcontrolset\services\storsvc\triggerinfo HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0 $$
                                            HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1 HKLM\system\currentcontrolset\services\svsvc
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\svsvc\triggerinfo HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0
                                            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\1 HKLM\system\currentcontrolset\services\swprv
Opens key
Opens key
Opens key
                                            HKLM\system\currentcontrolset\services\swprv\triggerinfo HKLM\system\currentcontrolset\services\sysmain
Opens key
                                            Opens key:
Opens key
                                            HKLM\system\currentcontrolset\services\systemeventsbroker
Opens key
                                            HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0
                                            HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1
Opens key:
                                            \label{thm:local} HKLM\system\currentcontrolset\services\systemevents broker\triggerinfo\2 HKLM\system\currentcontrolset\services\tabletinputservice
Opens key
Opens key:
Opens key:
Opens key:
                                            HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
Opens key
                                            \label{thm:local_ham} $$HKLM\system\currentcontrolset\services\tapisrv\triggerinfo}$$HKLM\system\currentcontrolset\services\termservice
Opens key
Opens key
                                            \label{thm:local} HKLM \system \current control set \services \terms ervice \trigger info HKLM \system \current control set \services \themes
Opens key
Opens key
Opens key:
                                            {\tt HKLM \ 'system \ 'current controlset \ 'services \ 'triggerinfo}
                                            HKLM\system\currentcontrolset\services\threadorder
Opens key
Opens key
                                            {\tt HKLM \colored \c
Opens key
                                            HKLM\svstem\currentcontrolset\services\timebroker
                                            HKLM\system\currentcontrolset\services\timebroker\triggerinfo
Opens key:
Opens key
                                            HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0
                                            HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1
Opens key:
Opens key
                                            HKLM\system\currentcontrolset\services\timebroker\triggerinfo\2
Opens key:
                                            HKLM\system\currentcontrolset\services\tlntsvr
Opens key
                                            HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo
Opens key
                                            HKLM\system\currentcontrolset\services\trkwks
```

```
Opens key
                                                 HKLM\system\currentcontrolset\services\trkwks\triggerinfo
Opens key:
                                                 HKLM\system\currentcontrolset\services\trustedinstalle
Opens key
                                                 HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo
                                                 HKLM\system\currentcontrolset\services\uiOdetect
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\ui0detect\triggerinfo HKLM\system\currentcontrolset\services\umrdpservice
Opens key
Opens key
Opens key
                                                 Opens key
                                                 HKLM\system\currentcontrolset\services\upnphost\triggerinfo HKLM\system\currentcontrolset\services\vaultsvc
Opens key
                                                 HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\vds\triggerinfo
                                                 HKLM\system\currentcontrolset\services\vmicheartbeat
Opens key
 Opens key
                                                 HKLM \ 's y stem \ 'current control set \ 's ervices \ 'vmicheart beat \ 'trigger in form \ 'trigger in fo
Opens key
                                                 HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0
 Opens key:
                                                 HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\1
Opens key
                                                 HKLM\system\currentcontrolset\services\vmickypexchange
Opens key
                                                 HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo
Opens key
                                                 Opens key:
Opens key
                                                 HKLM\svstem\currentcontrolset\services\vmicrdv
                                                 HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0
Opens key:
                                                 HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\1
Opens key:
Opens key:
                                                 HKLM\system\currentcontrolset\services\vmicshutdown
HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo
                                                 HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0 HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\1
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\vmictimesync
                                                 HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo
Opens key
                                                 Opens key:
Opens key
                                                 HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\1
Opens key:
                                                 HKLM\system\currentcontrolset\services\vmicvss
Opens key
                                                 HKLM\system\currentcontrolset\services\vmicvss\triggerinfo
Opens key:
                                                 HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0
Opens key
                                                 HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\1
                                                 HKLM\system\currentcontrolset\services\vss
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\vss\triggerinfo
Opens key:
                                                 HKLM\system\currentcontrolset\services\w32time
                                                 HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key
Opens key:
                                                 HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
                                                 HKLM\system\currentcontrolset\services\w32time\triggerinfo\1 HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wbengine
HKLM\system\currentcontrolset\services\wbengine\triggerinfo
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wbiosrvo
Opens key
                                                 HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
 Opens key
                                                 HKLM\system\currentcontrolset\services\wcmsvc
Opens key
                                                 HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo
Opens key:
                                                 HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0
                                                 HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\1
Opens key
 Opens key
                                                 HKLM\system\currentcontrolset\services\wcncsvc
Opens key
                                                 HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key:
                                                 HKLM\system\currentcontrolset\services\wcspluginservice
Opens key
                                                 \label{thm:local-hklm} HKLM \system \current controlset \services \swcspluginservice \trigger info HKLM \system \current controlset \services \swdiservice host
Opens key:
Opens key
                                                 HKLM\svstem\currentcontrolset\services\wdiservicehost\triggerinfo
Opens key:
                                                 HKLM\system\currentcontrolset\services\wdisystemhost
                                                 HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo HKLM\system\currentcontrolset\services\webclient
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\webclient\triggerinfo HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
                                                 HKLM\system\currentcontrolset\services\wecsvc
Opens key
                                                 HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
Opens key
                                                 HKLM\svstem\currentcontrolset\services\wersvc
                                                 HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key:
Opens key
                                                 HKLM\svstem\currentcontrolset\services\wersvc\triggerinfo\0
                                                 HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wiarpo
Opens key:
                                                 {\tt HKLM \ } system \verb| current control set \verb| services \verb| wiarpc \verb| trigger info \\
Opens key:
Opens key:
                                                 \label{thm:hklm} HKLM \system \current control set \services \winht tpaut oproxys \color \c
                                                 HKLM\system\currentcontrolset\services\winmgmt
HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\winrm
HKLM\system\currentcontrolset\services\winrm\triggerinfo
                                                 HKLM\system\currentcontrolset\services\wlansvc
HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
Opens key
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wlidsvc
HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo
Opens key
                                                 HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0
Opens key:
Opens key
                                                 HKLM\svstem\currentcontrolset\services\wlidsvc\triggerinfo\1
Opens key
                                                 HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\2
Opens key
                                                 HKLM\svstem\currentcontrolset\services\wmiapsrv
                                                 HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
Opens key:
Opens key
                                                 HKLM\system\currentcontrolset\services\wmpnetworksvc
Opens key:
                                                 HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
Opens key:
Opens key:
                                                 HKLM\system\currentcontrolset\services\wpcsvc
                                                 HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
Opens key
                                                 HKLM\system\currentcontrolset\services\wpdbusenum
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
                                                 \label{thm:local-problem} HKLM \system \current controlset \services \wpdbusenum \trigger in fold \\ HKLM \system \current controlset \services \wpdbusenum \trigger in fold \\ \end{tikzpicture}
Opens key
Opens key
                                                 \label{thm:local_ham} HKLM \system \current controlset \services \wpdbusenum \trigger in fold \system \current controlset \services \wpdbusenum \trigger in fold \system \sy
Opens key
Opens key
Opens key:
                                                 HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\5
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wsearch
Opens key
                                                 HKLM\svstem\currentcontrolset\services\wsearch\triggerinfo
                                                 HKLM\system\currentcontrolset\services\wsservice
Opens key:
Opens key
                                                 HKLM\system\currentcontrolset\services\wsservice\triggerinfo
                                                 HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0
Opens key:
Opens key
                                                 HKLM\system\currentcontrolset\services\wsservice\triggerinfo\1
Opens key:
                                                 HKLM\system\currentcontrolset\services\wuauserv
                                                 HKLM\svstem\currentcontrolset\services\wuauserv\triggerinfo
Opens key
Opens key
                                                 HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0
```

```
Opens key
                                                                       HKLM\system\currentcontrolset\services\wauserv\triggerinfo\1
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\2
    Opens key
                                                                       HKLM\system\currentcontrolset\services\wudfsvc
                                                                        HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
     Opens key:
    Opens key
                                                                       \label{thm:local_ham} HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0 HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1 \\
    Opens key
    Opens key
                                                                       HKLM\system\currentcontrolset\services\wansvc
HKLM\system\currentcontrolset\services\wansvc\triggerinfo
    Opens key:
    Opens key
                                                                       \label{thm:hkcusoftware} HKCU \ software \ clsses \ clsid \ \{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917\} \\ HKCR \ clsid \ 
    Opens key
Opens key:
e212013ea917}\treatas
                                                                       HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee
                                                                       HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\ \ treat as
                                                                       HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee
    Opens key
e212013ea917}\inprocser
                                                                       HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprocserver32
    Opens key:
                                                                        HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b
e212013ea917}\inprochandler32
    Opens key:
                                                                       Opens key
                                                                       HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4e6
e212013ea917}\inprochandler
                                                                       HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprochandler
    Opens kev:
                                                                       HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
     Opens key:
    Opens key
                                                                       HKCR\clsid\{c90250f3-4d7d-4991-9h69-a5c5hc1c2ae6}
                                                                       HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69
    Opens key:
a5c5bc1c2ae6}\treatas
                                                                       HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas
    Opens key:
    Opens key
                                                                       HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69
a5c5bc1c2ae6}\inprocserver32
                                                                       HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32
HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-
    Opens key:
    Opens key
a5c5bc1c2ae6}\inprochandler32
                                                                       HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32
    Opens key:
                                                                        HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69
a5c5bc1c2ae6}\inprochandler
    Opens key:
                                                                       Opens kev:
                                                                       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}\proxystubclsid32
    Opens kev:
                                                                       HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
                                                                       HKLM\software\policies\microsoft\windows\edgeui
     Opens key:
    Opens key
                                                                       HKCU\software\policies\microsoft\windows\edgeui
                                                                       HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
    Opens key
     Opens key
                                                                       HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
                                                                       HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805
    Opens key
5e9f541bd8c9}\proxystubclsid32
    Opens key:
                                                                       HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
                                                                       HKLM\system\currentcontrolset\enum\swd\printenum\printqueue
    Opens key
                                                                       HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{afd97640-86a3-4210-b67c-
289c41aabe55}\0002
    Opens kev:
HKLM \ system \ current control set \ enum \ swd \ printenum \ print queues \ properties \ \{afd 97640-86a 3-4210-b67c-86a 3-
289c41aabe55}\0003
    Opens key:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{a45c254e-df1c-4efd-8020-
67d146a850e0}\0011
Opens\ key: \\ \hline HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{8c7ed206-3f8a-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4827-b3ab-4
ae9e1faefc6c}\0002
                                                                       HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
    Opens key:
     Opens key
                                                                       {\tt HKLM} \verb|\software\policies\microsoft\windows\control\ panel\desktop|}
                                                                       HKCU\software\policies\microsoft\windows\control panel\desktop
    Opens key
                                                                       HKCU\software\microsoft\windows\currentversion\explorer\advanced
HKLM\software\microsoft\windows\currentversion\explorer\advanced
     Opens key:
    Opens key
                                                                       HKCU\software\microsoft\internet explorer\toolbar
HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}
     Opens key
    Opens key
                                                                        HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}
     Opens key
    Opens key
                                                                       HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\treatas
    Opens key:
                                                                       HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\treatas
    Opens key
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5a8b627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d46-4d65-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-4d64-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3ab627-92f3667-92f367-92f367-92f367-9667667-966767-966767-966767-966767-966767-966767-966767-966767-966767-96676-9667607-9667607-9667607-966
73626ae31971}\inprocserver32
                                                                       HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprocserver32
    Opens key:
    Onens key
                                                                       HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3
73626ae31971}\inprochandler32
                                                                       \label{eq:hkcr} HKCR\clsid\f5a8b627-4d46-4d65-92f3-73626ae31971\\\label{eq:hkcu} HKCU\software\classes\clsid\f5a8b627-4d46-4d65-92f3-
    Opens key:
     Opens key
73626ae31971}\inprochandler
                                                                       HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprochandler
    Opens key:
                                                                       HKLM\software\microsoft\windows\currentversion\explorer\commandstore
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\
    Opens key
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar
HKLM\software\microsoft\windows\currentyersion\explorer\commandstore\shell\windows.statusbar\
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{031e4825-7b94-4dc3-
b131-e946b44c8dd5}
    Opens key
                                                                       HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}
    Opens key:
                                                                       HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}
Opens key:
6ccfeeaa142a}\treatas
                                                                       HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
                                                                       \label{local-hkcr} HKCR\clsid\\ \{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a\\\} \treatas\\ HKCU\\software\\ classes\\ clsid\\ \{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a\\\} \treatas\\ HKCU\\ software\\ classes\\ clsid\\ treatas\\ description of the second of the se
    Opens key:
    Opens key
                                                                     er32
6ccfeeaa142a}\inprocser
                                                                       HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprocserver32
    Opens key:
                                                                       HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a
    Opens key
6ccfeeaa142a}\inprochandler32
    Opens key:
                                                                       HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprochandler32
    Opens key
                                                                       HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprochandler
    Opens key:
                                                                       HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprochandler
                                                                       HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
     Opens key:
    Opens key:
                                                                       HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
                                                                       HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d
    Opens key
ea55d8994f1a}\treatas
    Opens key:
                                                                        HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas
```

```
ea55d8994f1a}\inprocserver32
     Opens key:
                                                                           HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32
      Opens key:
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}
     Opens key:
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
     Opens key:
b8e8-d92d736469be}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
     Opens key
b8e8-d92d736469be}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003
Openskey: HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler32
                                                                           HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32
     Opens key:
                                                                           HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler
Opens key:
11e3-be67-0800272f6e60}
                                                                           Opens key:
                                                                           HKLM \ system \ current controls et \ control \ device containers \ \ \{623cc954-8780-1686, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 1886, 188
163-be7-0800272f6e60}\properties
Opens key: HKLM\system\currentcontrolset\control\devicecontainers\\\ 623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
     Opens key:
b8e8-d92d736469be}\properties\{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
                                                                           HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
     Opens key:
11e3-be67-0800272f6e60}
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
     Opens key:
b32c-cd2da77617c7}
                                                                           HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler
     Opens key:
                                                                           HKCU\software\classes\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
       Opens key:
     Opens key:
                                                                            \label{lem:hklm} \verb+Kklm/system/currentcontrolset/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-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4944-e0b1-4
b8e8-d92d736469be}\properties\{3b2ce006-5e61-4fde-bab8-9b8aac9b26df}\0001
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties
                                                                           Opens key:
b32c-cd2da77617c7}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002
                                                                           HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
     Opens key:
     Opens kev:
                                                                           HKCR\clsid\{h8967f85-58ae-4f46-9fh2-5d7904798f4h}
     Opens key:
                                                                           HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\treatas
                                                                           HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\treatas
     Opens key:
Opens key: HKCI
5d7904798f4b}\inprocserver32
                                                                           HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
                                                                           HKLM \ system \ current control set \ enum \ swd \ printenum \ \{af 023001-e0b1-4934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b14934-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b1494-b14
b8e8-d92d736469be}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011
Opens key: HKLM\syste
11e3-be67-0800272f6e60}\properties
                                                                           HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
Opens key: HKLM\system\currentcontrolset\control\devicecontainers\\\\ 623cc955-8780-11e3-be67-0800272f6e60\\properties\\\\ 3464f7a4-2444-40b1-980a-e0903cb6d912\\\ 000a
     Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 1414 008d ffffffff fffffff 0^ccc77560bc3634a486857716562968286
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\deviceupdatelocations
                                                                           HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
     Opens key:
     Opens key:
                                                                           HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
     Opens key
a2dd-08002b30309d}
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-
 a2dd-08002b30309d}
                                                                           HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-
     Opens kev:
08002b30309d}\shellfolder
                                                                           HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}\shellfolder
     Opens kev:
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003
                                                                           HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
     Opens key:
b32c-cd2da77617c7}\properties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011
     Opens key:
                                                                           b32c-cd2da77617c7\\properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\\0002
                                                                           HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprocserver32
     Opens key:
Opens key: HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-b32c-cd2da77617c7}\properties\{3b2ce006-5e61-4fde-bab8-9b8aac9b26df}\0001
Opens key: HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-b32c-cd2da77617c7}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011
HKLM \system \corrent control \system \control \system 
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd rvi0001 agnieszka
01_1d_07d7_b2_1414_008d_ffffffffffffffffff0^700ef59a5da31cbd79f31237af2ad4c4
     Opens key
HKL\dot{M} \\ \text{Syst\'em} \\ \text{current control set } \\ \text{control } \\ \text{graphics drivers} \\ \text{configuration} \\ \text{msho62e0\_00\_07db\_c6^182fdc0875f0a76803e4a9848a8c1ea7} \\ \text{drivers} \\ \text{drivers}
     Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{21ec2020
3aea-1069-a2dd-08002b30309d}\shellfolder
     Opens kev:
                                                                           HKLM\software\microsoft\windows\currentversion\explorer\clsid\{21ec2020-
3aea-1069-a2dd-08002b30309d}\shellfolder
     Onens key
                                                                           HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2
5d7904798f4b}\inprochandler32
                                                                           HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprochandler32
     Opens key:
Opens key:
                                                                           HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprochandler
     Opens key:
                                                                           HKCR \verb|\clsid|{b8967f85-58ae-4f46-9fb2-5d7904798f4b} \verb|\inprochandler| and the state of the st
     Opens key:
HKCU\software\microsoft\windows\currentversion\policies\nonenum
HKLM\software\microsoft\windows\currentversion\policies\nonenum
     Opens key:
     Opens kev:
      Opens key
                                                                           HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
     Opens key
                                                                           HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
      Opens key:
49b9-88dd-029876e11c01}
     Opens key:
 49b9-88dd-029876e11c013
     Opens key:
```

Opens key

HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-

```
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00
                                                                                                                             HKLM\software\microsoft\windows\currentversion\policies\explorer
         Opens key:
        Opens key
                                                                                                                             HKCU\software\microsoft\windows\currentversion\policies\explorer
         Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
        Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
        Opens key:
Opens key
HKLM \ software \ microsoft \ windows \ current version \ explorer \ my computer \ names pace \ delegate folders \ \ 35786d3c-1000 \ names \
b075-49b9-88dd-029876e11c01}
        Opens key:
                                                                 e\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{9113a02d-
00a3-46b9-bc5f-9c04daddd5d73
        Opens key:
HKLM \label{eq:hklm} KLM \label{eq:hklm} HKLM \label{eq:hklm} Software \label{eq:hklm} windows \label{eq:hklm} Current \label{eq:hklm} Very \label{eq:hklm} White \label{eq:hkklm} White \label{eq:h
02f0-451e-9a26-ae317cfd7779}
       Opens key:
 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:
Opens key:
\label{two-policy} HKCU \software \microsoft \windows \current version \explorer \session in follow y computer \names pace \delegate folders \names \names
        Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace
        Opens key:
\label{thm:hkcu} \begin{tabular}{ll} HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volumebrane \columnwidth) and the property of 
       Opens key:
 HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \{d5291c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c88-1c64-7c8
11e3-be65-806e6f6e6963}\
         Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders
        Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userslibraries\namespace
        Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders\{896664f7-
 12e1-490f-8782-c0835afd98fc}
        Opens key:
                                                                                                                             HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
                                                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
        Opens key:
        Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{9c73f5e5-7ae7-
4e32-a8e8-8d23b85255bf}
        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:hammespace} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\l\userslibraries\namespace} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\l\userslibraries\namespace} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\l\userslibraries\namespace} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\l\userslibraries\namespace} \parbox{$HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\l\userslibraries\namespace\explorer\sessioninfo\namespace\explorer\sessioninfo\namespace\explorer\sessioninfo\namespace\explorer\sessioninfo\namespace\explorer\sessioninfo\namespace\explorer\sessioninfo\namespace\explorer\sessio
        Opens kev:
Opens kev:
                                                                                                                           HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder
        Opens kev:
                                                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
        Opens key:
                                                                                                                             7ae7-4e32-a8e8-8d23h85255hf3\shellfolder
       Opens key:
                                                                                                                             HKLM \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{9c73f5e5-microsoft\} \ description 
7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32
        Opens key:
                                                                                                                             {\tt HKLM \coftware \cosoft \windows \current \version \cosoft \windows \corrent \cosoft \coso
                                                                                                                             HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
        Opens key:
         Opens key:
                                                                                                                             \label{thm:linear} \mbox{HKCU\software\mbox{\sc windows\currentversion\shell extensions\cached} \\
        Opens key
                                                                                                                             HKLM\software\microsoft\windowsruntime\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf)
                                                                                                                             HKCR\activatableclasses\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
        Opens kev:
                                                                                                                             HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
        Opens key:
8d23b85255bf}\treatas
        Opens key:
                                                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\treatas
        Opens key
                                                                                                                             HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32
        Opens kev:
                                                                                                                             HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprochandler32
        Opens key:
                                                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler32
        Opens key:
                                                                                                                             HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprochandler
                                                                                                                             HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler
        Opens key:
a8e8-8d23b85255bf}
                                                                                                                             HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
        Opens key:
                                                                                                                           HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
         Opens key
        Opens key
3aea-1069-a2d8-08002b30309d}
       Opens kev:
                                                                                                                             HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\
       Opens kev:
                                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellex\iconhandler
       Opens kev:
                                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\defaulticon
        Opens key
\label{thm:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \hidedesk topic ons \new start panel \end{tabular}
Opens\,key;\\ HKLM\software\mbox{\tt microsoft\windows\currentversion\explorer\hidedesktopicons\newstartpanel}
        Opens key:
HKCU \label{twindows} \label{twindows} HKCU \label{twindows} \label{twindows} Label{twindows} HKCU \label{twindows} \label{twindows} \label{twindows} \label{twindows} \label{twindows} HKCU \label{twindows} \label{twindows} \label{twindows} \label{twindows} \label{twindows} \label{twindows} HKCU \label{twindows} \la
                                                                                                                           HKCU\software\classes\clsid\\603d3801-bd81-11d0-a3a5-00c04fd706ec}
HKCR\clsid\\603d3801-bd81-11d0-a3a5-00c04fd706ec}
        Opens key:
        Opens key:
                                                                                                                             HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a
        Opens key
00c04fd706ec}\treatas
        Opens key:
                                                                                                                             HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\treat as the control of the c
        Opens kev:
                                                                                                                             HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32
        Opens kev:
                                                                                                                             HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32
                                                                                                                             HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
         Opens key:
00c04fd706ec}\inprochandler32
                                                                                                                             HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler32
        Opens key:
        Opens key
                                                                                                                             HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5
00c04fd706ec}\inprochandler
```

```
Opens key
                                                                       HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler
                                                                       HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
     Opens key:
    Opens key:
                                                                       HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
                                                                       HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae
     Opens key
355b7f55341b}\treatas
                                                                       HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
    Opens key:
Opens key: HKCI
355b7f55341b}\inprocserver32
                                                                       HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
                                                                       HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
    Opens key:
                                                                       HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
    Opens key
355b7f55341b}\inprochandler32
                                                                       HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
    Opens key:
     Opens key
                                                                       HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae
355b7f55341b}\inprochandler
                                                                       Opens key:
    Opens key:
                                                                       HKCU\software\classes\applications\calc.exe
     Opens key:
                                                                       HKCR\applications\calc.exe
                                                                       HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
    Opens key
                                                                       HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
     Opens key
    Opens key
                                                                       HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\treatas
    Opens kev:
                                                                       HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{317d06e8-5f24-433d-bdf7-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-64443d-644443d-64443d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-6444d-6444d-64444d-64444d-6444d-64444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-6444d-64444d-6444d-64444d-6444d-6444d-6444d-6444d-6444d-64444d-64444d-64444d-6444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-644444d-64444d-64444d-64444d-64444d-644444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-64444d-6444d-64444d-64444d-64444d-64444
    Opens key
79ce68d8abc2}\inprocserver32
                                                                       HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32
    Opens key:
    Opens key
                                                                       HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler32
    Opens key:
                                                                       HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler32
                                                                       HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
    Opens key
79ce68d8abc2}\inprochandler
                                                                       HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler
    Opens key:
                                                                       \label{thm:hkcusoftware} HKCU software \clsid {6f13dd2e-ebee-4dd5-a72e-850b2087f5dd} \\ HKCR \clsid {6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}
    Opens key:
                                                                       HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e
850b2087f5dd}\treatas
    Opens key:
                                                                       HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\treatas
    Opens key
                                                                       HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprocser
                                                                    er32
                                                                       HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32
    Opens key:
     Opens key
                                                                       HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprochandler32
                                                                       HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler32
    Opens key:
    Onens key
                                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{6f13dd2e - ebee - 4dd5 - a72e^{-1}\} + (13dd2e - ebee - 4dd5 - a72e^{-1}) + (13dd2e 
850b2087f5dd}\inprochandler
                                                                       HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler
    Opens key:
    Opens key:
HKL\ M \ software \ microsoft \ windows \ current version \ photoproper tyhandler \ container associations
    Opens key:
                                                                       HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
    Opens key:
                                                                       HKLM\software\microsoft\windowsruntime\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}
                                                                       HKCR\activatableclasses\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
    Opens kev:
                                                                       HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
     Opens key
                                                                       HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
    Opens kev:
     Opens key:
                                                                       HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b
323e85a1ce84}\treatas
    Opens key:
                                                                       HKCR \verb|\clsid| \{9 dac2c1e-7c5c-40eb-833b-323e85a1ce84\} \verb|\treatas| \} treatas| A substitution of the subs
    Onens key
                                                                       HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b
323e85a1ce84}\inprocserver32
    Opens key:
                                                                       HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
                                                                       HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b
    Opens key
323e85a1ce84}\inprochandler32
                                                                       HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
    Opens key:
     Opens key:
                                                                       HKCU\software\classes\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{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \begin{tabular}{ll} PKCU \label{thm:local_hammon} Software \begin
Opens key:
settings\zones\1
                                                                       \label{local-observation} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
    Opens key:
                                                                       \label{local-observation} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings\zones\2
    Opens key:
                                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
    Opens key:
                                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
    Opens key:
                                                                       HKCU\software\policies\microsoft\internet explorer
    Opens key:
                                                                       HKCU\software\microsoft\internet explorer\security HKLM\software\microsoft\internet explorer\security
    Opens key:
                                                                       HKCIJ\software\microsoft\windows\currentversion\internet settings\zones
    Opens key:
                                                                       HKLM\software\microsoft\windows\currentversion\internet settings\zones
    Opens key:
\label{lem:constant} Opens~key: $$ HKLM\software\microsoft\windows\currentversion\action center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}$
    Opens key:
                                                                       HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{ca236752 - 2e77 - 4386 - b63b - b6
0e34774a413d}
                                                                       \label{local-continuity} HKCR\activatable classes \clsid \ \{ca236752-2e77-4386-b63b-0e34774a413d\} \\ HKCU\software \classes \clsid \ \{ca236752-2e77-4386-b63b-0e34774a413d\} \\
    Opens key:
    Opens key:
                                                                       HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
     Opens key
                                                                       HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b
    Opens key
0e34774a413d}\treatas
                                                                       HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
    Opens kev:
                                                                       HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b
0e34774a413d}\inprocserver32
    Opens key:
                                                                       HKCR \verb|\clsid|{ca236752-2e77-4386-b63b-0e34774a413d} \verb|\inprocserver32| \\
    Opens key
                                                                       HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b
0e34774a413d}\inprochandler32
    Opens key:
                                                                       HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
     Opens key
                                                                       HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b
```

```
0e34774a413d}\inprochandler
                                                                        HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
     Opens key:
     Opens key
                                                                        HKLM\software\microsoft\wbem\cimom
                                                                        HKLM\software\policies\microsoft\windows\windows error reporting
     Opens key:
    Opens key:
                                                                        {\tt HKLM \backslash software \backslash microsoft \backslash windows \backslash 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\ere
    Opens key
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \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:
                                                                         HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
    Opens key
                                                                        HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32
    Opens kev:
                                                                        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:
                                                                        HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
                                                                        HKLM\software\microsoft\msxm160
     Opens key:
    Opens key:
                                                                        HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus action
center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
                                                                        HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3be-belle + belle + belle
499afcec98c4}
    Opens key:
                                                                         HKCR\activatableclasses\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
    Opens key
                                                                        HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
     Opens key:
                                                                         HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
    Opens key
                                                                        HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be
499afcec98c4}\treatas
    Opens key:
                                                                        HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
    Opens key:
                                                                        HKCU \setminus software \setminus classes \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3be - beta \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - 4053 - a3be - beta \setminus c8e6f269 - b90a - beta \setminus c8e6f269 - beta
499afcec98c4}\innrocserver32
                                                                        HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
    Opens key:
    Opens key
                                                                        \label{local-eq:hkcu-software-classes-clsid-calc} HKCU \setminus software \setminus classes \setminus clsid \setminus \{c8e6f269 - b90a - 4053 - a3ber + beream 
499afcec98c4}\inprochandler32
    Opens key:
                                                                       HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
    Opens key:
499afcec98c4}\inprochandler
                                                                        HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
    Opens key:
     Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
                                                                        HKLM\software\microsoft\windows\currentversion\policies\system
    Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action
    Opens kev:
center\providers\com\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
    Opens kev:
                                                                        HKLM\software\microsoft\windowsruntime\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}
    Opens kev:
                                                                        HKCR\activatableclasses\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
                                                                        HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
    Opens key:
    Opens key
                                                                        HKCR\clsid\{088e8dfh-2464-4c21-had2-f0aa6dh5d4hc}
                                                                        HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2
    Opens key
f0aa6db5d4bc}\treatas
                                                                        HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas
    Opens key:
    Opens key
                                                                        HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprocserver32
                                                                        HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32
    Opens key:
                                                                        HKLM \setminus software \setminus microsoft \setminus windows runtime \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-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-4a5
    Opens key:
40cd513679d5}
                                                                        HKCR\activatableclasses\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
    Opens kev:
                                                                        HKCU\software\classes\clsid\\900c0763-5cad-4a34-bc1f-40cd513679d5\}
HKCR\clsid\\900c0763-5cad-4a34-bc1f-40cd513679d5\}
     Opens key
    Opens kev:
                                                                         HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc
40cd513679d5}\treatas
    Opens key:
                                                                         Opens key
                                                                        HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprochandler32
    Opens key:
                                                                        HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler32
    Opens key:
                                                                        HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32
                                                                        HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
    Opens key:
Opens key: HK
f0aa6db5d4bc}\inprochandler
                                                                        HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2
                                                                        HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler
    Opens key:
                                                                        HKLM\software\policies\microsoft\windows\system
    Opens key:
                                                                        HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
    Opens key
40cd513679d5}\inprochandler32
                                                                        HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
    Opens key:
    Opens key
                                                                        HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprochandler
                                                                        HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler
    Opens kev:
     Opens key:
                                                                        HKLM \verb|\software\m| icrosoft \verb|\windows\currentversion\explorer| \\
    Opens key:
                                                                        HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
    Opens key:
                                                                        HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
                                                                        HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
    Opens key:
Opens key: HKCU\
00aa00404770}\proxystubclsid32
                                                                        HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-
                                                                       \label{thm:linear} HKCR\interface \ \{b722bccb-4e68-101b-a2bc-00aa00404770\}\ proxystubclsid32\ HKLM\software\ microsoft\ windows runtime\ clsid \ \{a4a1a128-768f-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0-bf75-41e0
    Opens key:
    Opens key:
e4fddd701cba)
                                                                        HKCR\activatableclasses\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
    Opens key:
                                                                        HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
HKLM\software\microsoft\windowsruntime\clsid\{d26de5c1-c061-43f7-9c40-
     Opens key
    Opens key
7517526cf1c1}
                                                                        HKCR\activatableclasses\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
    Opens kev:
                                                                         HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
      Opens key:
    Opens kev:
                                                                        HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
     Opens key:
                                                                        7517526cf1c1}\treatas
                                                                         HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas
    Opens key:
     Opens key
                                                                        HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
     Opens key
                                                                        HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
```

```
e4fddd701cba}\treatas
   Opens key
                                       HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
  Opens key
                                      HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba)
  Opens key:
                                      HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
                                      HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40
   Opens key
7517526cf1c1}\inprocser
                                      er32
  Opens key:
                                      HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32
  Onens key
                                      HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf7
e4fddd701cba}\inprochandler32
  Opens key:
                                      HKCR \verb|\clsid| \{a4a1a128-768f-41e0-bf75-e4fddd701cba\} \verb|\inprochandler32| \} (a4a1a128-768f-41e0-bf75-e4fddd701cba) | A control of the contr
                                      HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75
  Opens key
e4fddd701cba}\inprochandler
                                      HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
  Opens key:
7517526cf1c1}\inprochandler32
                                      HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler32
  Opens key:
                                      HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c4
7517526cf1c1}\inprochandler
                                      HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler
HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
  Opens key:
  Opens key
                                       HKCU\software\microsoft\windows\currentversion\startupnotify
   Opens key
  Opens key
                                      HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Onens key
                                      HKLM\software\microsoft\windowsruntime\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3}
  Opens key:
Opens key:
                                      HKCR\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
                                      HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key
                                      HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key
                                      HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3)
                                      HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key:
   Opens key
                                      HKCU\software\classes\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3
  Opens key:
  Opens key
                                      HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
  Opens kev:
                                      HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
  Opens key
                                      HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
  Opens kev:
                                      HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
Opens key: HKLM\software\microsoft\windows\currentvecenter\providers\eventlog\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}
Opens key: HKLM\software\microsoft\windows\currentversion\action center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
Opens key: HKLM\software\microsoft\windows\current\center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
Opens key: HKLM\software/microsoft/windows/currentversion\action center\providers\eventlog\{b447b4db-7780-11e0-ada3-18a90531a85a}
                                      HKLM\software\microsoft\windows\currentve
  Opens key
center\providers\eventlog\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\action
center \verb|\providers| eventlog \verb|\{2374911b-b114-42fe-900d-54f95fee92e5\}|
  Opens key:
                                      HKLM\software\microsoft\windows\currentver
center\providers\eventlog\{96f4a050-7e31-453c-88be-9634f4e02139}
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\action center
                                      Opens key:
  Opens key
  Opens key
                                      HKLM \verb|\software\microsoft\windows| nt\current version \verb|\profilelist\s-1-5-20| |
                                      HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
  Opens key
shell folders
                                      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 kev:
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sppsvc.exe
  Opens key:
                                       HKLM\system\currentcontrolset\control\session manager\quota system\s-1-
5-20
  Opens key
                                       HKLM\software\microsoft\ole
                                      HKLM\software\microsoft\ole\tracing
  Opens key
  Opens key:
                                       HKLM\system\currentcontrolset\control\mui\settings
  Opens key:
Opens key:
                                      HKLM\software\microsoft\oleaut
                                      HKLM\software\classes
                                      HKCR\appid\sppsvc.exe
  Opens key
                                      HKLM\system\currentcontrolset\services\http
  Opens key
Opens key:
nt\currentversion\softwa
                                      HKLM\software\microsoft\windows
                                      reprotectionplatform
  Opens key
                                      HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong
cryptographic provider
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10
  Opens key
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12
   Opens key:
   Opens key
   Opens key:
                                       HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13
  Opens key
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14
                                       HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15
   Opens key:
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16
   Opens key
  Opens key:
                                       HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17
  Opens key:
Opens key:
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19
  Opens key
                                      \label{eq:hklmsystem} \begin{tabular}{ll} HKLM\system\pa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\\ HKLM\system\pa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20\\ \end{tabular}
  Opens key
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22
  Opens key
                                      \label{eq:hklm-system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23} \\ \text{HkLM-system-wpa-8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24} \\
  Opens key
  Opens key:
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26
  Opens key:
   Opens key
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28
   Opens key
  Opens key
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30
   Opens key:
   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
                                      HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33
   Opens key
```

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

Opens key

```
Opens key
                                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5
                                                                           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6
     Opens key:
                                                                          \label{eq:hklmsystemwpa8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7} \\ \text{HkLM} system \\ \text{wpa} \\ \text{8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8} \\
     Opens key
     Opens key:
     Opens key
                                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9
                                                                          HKCU\software\microsoft\windows
     Opens key
\label{lem:nt-current-version-soft-wave-protection-platform-persisted transform-persisted transform-pers
nt\currentve
                                       sion\softwareprotectionplatform\persistedsystemstate
    HKLM\software\microsoft\windows
     Opens key
nt\currentversion\softwareprotectionplatform\plugins\modules
Opens key: HKLM\software\microsoft\windows
nt\currentve
                                                                         reprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-12006ef9b32a
                                                                          HKLM\software\microsoft\windows
    Opens key:
nt\currentve
                                                                          reprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662
    Opens key:
                                                                          HKLM\software\microsoft\windows
nt\currentv
                                                                          reprotectionplatform\plugins\objects
     Opens key:
                                                                          HKLM\software\microsoft\window
                                                                          reprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0
nt\currentve
    Opens key
                                                                          HKLM\software\microsoft\window
                                                                         reprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0
nt\currentversio
    Opens kev:
                                                                          HKLM\software\microsoft\window
nt\currentve
                                       sion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0
     Onens key
                                                                          HKI M\software\microsoft\windov
nt \verb|\currentversion| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/hwid/4.0| | the property of the 
     Opens key
                                                                          HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0
     Opens key
                                                                          HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
     Opens key:
                                                                          HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009
                                                                          HKLM\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect
     Opens key:
                                                                          HKLM\software\microsoft\windows
\label{lem:nt-current-version-software-protection-platform-plugins-objects-msft:rm/algorithm/vmd/1.0 \\ Opens key: HKLM\software\microsoft\windows
\label{lem:ntcurrent} $$ nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0 $$ Opens\key: HKLM\software\microsoft\windows $$
\label{lem:ntcurrent} $$nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0 $$ Opens key: $$HKLM\software\microsoft\windows
\label{lem:nt-current-version-software-protection-plugins-objects-msft:spp/action/kernel/1.0} Opens key: \\ HKLM\software\microsoft\windows
nt\currentve
                                                       software protection platform \verb|\plugins\>| objects \verb|\msft:spp/action/reeval/1.0| \\
                                                                          HKLM\software\microsoft\windows
     Opens key:
nt\currentversion
                                                      .softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0
HKLM\software\microsoft\windows
     Opens key:
nt\currentv
                                                                        reprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0
     Opens key:
                                                                          HKLM\software\microsoft\windows
                                                                          reprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0
nt\currentve
     Opens key
                                                                          HKLM\software\microsoft\window
nt\currentve
                                                                          reprotectionplatform\plugins\objects\msft:spp/collector/global/1.0
     Opens kev:
                                                                          HKLM\software\microsoft\window
                                                                          reprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0
nt\currentve
    Opens kev:
                                                                          HKLM\software\microsoft\window
nt\currentver
                                       Opens kev:
                                                                          HKLM\software\microsoft\window
\verb|nt\currentversion\software| protection platform \verb|plug| ins\objects \verb|msft:spp/licenseacquisition/payload | platform of the platform of th
     Onens key
                                                                          HKI M\software\microsoft\windov
nt `current version `software protection platform `plugins `objects `msft: spp/license acquisition/payload handler/pkc/1.0 acquisition of the protection o
     Opens key
                                                                          HKLM\software\microsoft\window
nt \verb|current| version \verb|software| protection platform \verb| plugins \verb| objects \verb| msft:spp/licenseacquisition/payload | handler/rac/1.0 | like the protection of the protection
                                                                          HKLM\software\microsoft\window
     Opens key
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0
     Opens key:
                                                                          HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0
Opens key: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey
                                                                          HKLM\software\microsoft\windows
     Opens key:
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
                                                                          HKLM\software\microsoft\windows
     Opens key
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0 Opens key: HKLM\software\microsoft\windows
\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
\label{lem:nt-current-version-software-protection-plugins-objects-msft:spp/windowsfunctionality/agent/7.0 \\ Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
     Opens key
                                                                          HKLM\software\microsoft\com3
     Opens key
                                                                          HKCR\interface\{00000134-0000-0000-c000-00000000046} 
HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32
     Opens key
     Opens key
     Opens key
                                                                          HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
                                                                          HKLM\software\microsoft\windows nt\currentversion\
     Opens key:
                                                                          HKLM\svstem\setup\status
     Opens key
                                                                          HKCU\software\microsoft\windows
     Opens key
nt\currentversion\softwareprotectionplatform\reboot.sl brt commit
                                                                          HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0
     Opens key:
     Opens key
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 1237&subsys 00000000&rev 02\3&267a616a&1&00
     Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08
     Opens key:
                                                                          Opens key
                                                                          HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0
     Opens key
                                                                          HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0
                                                                          HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0
     Opens key
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1
                                                                          HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0
     Opens key:
                                                                          HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0
     Opens key:
     Opens key
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 7111&subsys 00000000&rev 01\3&267a616a&1&09
     Opens key:
                                                                          HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0
     Opens kev:
HKLM\system\currentcontrolset\enum\ide\diskhitachi
                                                                                                                                                                                                                                                           1.0.7.3 \5&34baf594&0&0.0.0
                                                                          HKLM\system\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 key
                                                                          HKLM\svstem\wpa\
     Opens key
                                                                          HKLM\system\wpa\478c035f-04bc-48c7-b324-2462d786dad7-5p-9\
```

```
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10\
     Opens key:
                                                          Opens key
     Opens key:
    Opens key
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14\
    Opens key
    Opens key:
Opens key:
                                                          \label{eq:hklmsystem} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16\\ \label{eq:hklmsystem}
    Opens key
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18\
    Opens key
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\
    Opens key
    Opens key
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21\
    Opens key
    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\
                                                          \label{local-equation} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\\ \label{local-equation} \end{subarray}
     Opens key
     Opens key:
    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\
    Opens key
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30\
    Opens key:
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31\
    Opens key:
Opens key:
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33\
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5\
    Opens key
    Opens key
                                                          HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6\
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7\
     Opens key
    Opens key
     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}
    Opens kev:
                                                          HKCR\activatableclasses\clsid
     Opens key:
                                                          HKCR\activatableclasses\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
    Opens key
                                                          HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
                                                          HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\treatas
     Opens key:
                                                          HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32
    Opens key
                                                          HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler32
    Opens key:
    Opens key
                                                          HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler
                                                          HKLM\software\microsoft\windows\windows error reporting\wmm
    Opens key
     Opens key
                                                          HKCU\control panel\international
                                                          HKLM\software\microsoft\windowsruntime\clsid\{88d96a08-f192-11d4-a65f-
    Opens key
0040963251e51
                                                          HKCR\activatableclasses\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
    Opens key:
     Opens key:
                                                          HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\treatas
    Opens key
     Opens key:
                                                          HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32
HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler32
    Opens key
     Opens key
                                                          HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler
                                                          \label{thm:local} HKLM \system \controlset \control \cryptography \configuration \controlset \control \cryptography \configuration \cryptography \configuration \cryptography \configuration \cryptography \cryptography \configuration \cryptography \cryptograph
    Opens key
     Opens key:
    Opens key
                                                          HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-
 73e6154572dd)
   Opens key:
Opens key:
                                                          HKCR\activatableclasses\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
                                                          HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
                                                          HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32
     Opens key
    Opens key
                                                          \label{local-equation} HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\windows and left algorithms are supported by the control of the co
    Opens key
    Opens key:
     Opens key:
                                                          {\tt HKLM \ } system \verb| `current control \verb| set \verb| `control \verb| `product options | for the product of the produc
                                                          \label{thm:hklm} HKLM \system \current control set \control \terminal server [tsapp compat] \\ HKLM \system \current control \terminal server [tsuser enabled] \\
    Queries value
     Queries value
     Oueries value
 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \policies \microsoft \windows \safer \code identifiers \cite{transparentenabled} \end{tabular}
    Oueries value:
                                                          HKLM\system\currentcontrolset\control\nls\customlocale[emptv]
     Queries value
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
    Queries value:
    Oueries value:
                                                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
    Oueries value:
                                                          \label{local-operator} $$HKCU\control panel\desktop[preferreduilanguages] $$HKCU\control panel\desktop\muicached[machinepreferreduilanguages]$$
     Queries value:
     Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
                                                          HKLM\system\currentcontrolset\control\nls\sorting\versions[] HKCU\software\microsoft\windows
    Queries value:
     Queries value
 nt\currentversion\appcompatflags[showdebuginfo]
                                                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:
    Queries value:
                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
    Queries value:
options\dllnxoptions[26ec828da6d2651f90c74cb275b800cc.exe]
                                                          HKLM\software\microsoft\windows
    Queries value
nt\currentversion\gre_initialize[disablemetafiles]
                                                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[26ec828da6d2651f90c74cb275b800cc]
Queries value: HKLM\software\wow6432node\microsoft\windows
\verb|nt\currentversion\windows[loadappinit_dlls]| \\
    Queries value:
                                                          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Queries value:
Queries value:
                                                          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] HKLM\software\wow6432node\microsoft\direct3d[disablemmx]
                                                          HKLM\software\microsoft\sqmclient\windows[ceipenable] HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
    Queries value:
     Queries value:
     Oueries value:
                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \shell \end{tabular}
 folders[cache]
                                                          \label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc mage file execution} \\
options\dllnxoptions[untfs.dll]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
                                                          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]
                                                          HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
     Queries value:
    Oueries value
```

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

HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1\

Opens key

Queries value HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Oueries value $\label{thklm} HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ [next_catalog_entry_id]$ Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Oueries value ARKLMNsystem\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem] Queries value HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000002[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000003[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000004[packedcatalogitem] $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000006 \ [packed catalog item]$ $HKLM \setminus system \setminus current control set \setminus services \setminus winsock2 \setminus parameters \setminus protocol_catalog \mid catalog_entries \setminus 0000000000008 [packed catalog item]$ Queries value: Queries value: Queries value $\label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} winsock 2 \parameters \namespace_catalog 5 [serial_access_num] \\ \end{tabular} access_num \end{tabular} access_nu$ Queries value $HK\dot{L}M \land system \land current control set \land services \land winsock 2 \land parameters \land names pace_catalog5[num_catalog_entries]$ Queries value: Queries value $HKL\\ M\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries\space\namespace_catalog 5\catalog_entries\space\namesp$ Oueries value $HKL\ Mk system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000001 \ [providerid]$ Oueries value Oueries value Oueries value Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[version] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[storesserviceclassinfo] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[providerinfo] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[librarypath] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[displaystring] $HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ name space_catalog 5 \ \ catalog_entries \ \ 000000000002 [providerid]$ HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily] Queries value: 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 Oueries value $HKL\\ M (system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names pace_catalog 5 \catalog_entries \names \na$ Oueries value $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ (catalog_entries \ 000000000000003 \ (displaystring)) \ (displaystring) \ (di$ Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[providerid] Oueries value $HKL\\ M\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries\space\names family]$ Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[enabled] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version] Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[providerinfo] Queries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000004flibrarypath1 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[addressfamily] Queries value: $HKLM \system \verb|\currentcontrolset\services| winsock 2 parameters \verb|\namespace_catalog5| catalog_entries \symbol{0}00000000004 [supported namespace]|$ Queries value Oueries value

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000005[librarypath]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005[addressfamily]

Oueries value

Oueries value

Oueries value

Queries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace] Oueries value HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000005fenabled Oueries value Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005[providerinfo] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006[librarypath] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[displaystring] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[addressfamily] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006fversion1 Queries value: Queries value $HKL\ M \ system \ current controls et\ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 10000000000006 [providerinfo]]$ Queries value $\label{local-observation} HKLM \xspace{LM} in sock 2 \parameters [ws 2_32 numhandle buckets] \\$ HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Oueries value $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} winsock [max sock addrlength] \end{tabular}$ Oueries value $\label{local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} a meters \end{tabular} $$ in sock [used elayed acceptance] $$ in sock [used elayed$ Oueries value provider v1.0[type] Queries value: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \begin{tabul$ provider v1.0[image path] Queries value . HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems] Queries value: $\label{thm:local_ham} \begin{tabular}{ll} HKLM \label{thm:local_hamiltonian} HKLM \l$ HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] Queries value: HKLM\software\microsoft\cryptography[machineguid] Queries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\windows[displayversion] HKCU\control panel\desktop[paintdesktopversion] Oueries value: Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: $\label{thm:local_computername} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ is the computername (computername) $$ is the compu$ HKLM\system\setup[oobeinprogress]
HKLM\system\setup[systemsetupinprogress] Oueries value: Queries value: Oueries value: HKLM\software\microsoft\rpc[idletimerwindow] HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[current protocol catalog] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\000000000010[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\0000000000009fpackedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries64\000000000008fpackedcatalogitem1 Queries value Queries value: Queries value $HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog9 \catalog_entries 64 \noone00000000004 \[packed catalog item] \end{subarray}$ Oueries value $HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog9 \catalog_entries 64 \noone00000000003 \[packed catalog item] \end{subarray}$ Oueries value Oueries value Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog] Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries64\000000000006[providerid] Oueries value Oueries value Queries value Queries value Queries value: Queries value: $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} If the limit \label{limi$ cryptographic provider v1.0[type] $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} If the limit \label{limi$ Queries value cryptographic provider v1.0[image path]

Queries value: HKLM\software\microsoft\windows nt\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] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)] Oueries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] Queries value HKLM\software\microsoft\windows\currentversion[programw6432dir]

```
Queries value:
                                  HKLM\software\microsoft\windows\currentversion[commonw6432dir]
  Queries value
                                  HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
                                  HKU\.default\software\microsoft\windows\currentversion\explorer\user
  Queries value
shell folders[appdata]
  Oueries value
                                  HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundll32.exe[usefilter]
  Queries value
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[debugger]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundll32.exe[uselargepages]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundl132.e
                                  options]
  Queries value
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[dis
                                 ablewakecharge]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value
options\rundll32.exe[mitigationoptions]
  Queries value
\label{local_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ idebyside[preferexternal manifest] $$
 Oueries value
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[disableheaplookaside]
  Oueries value
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundl132.exe[frontendheapdebugoptions]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundl132.exe[shutdownflags]
  Queries value
                                  \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the
options\rundll32.exe[unloadeventtracedepth]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[tracingflags]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[minimumstackcommitinbytes]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[breakoninitializeprocessfailure]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundl132.exe[keepactivationcontextsalive]
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value
options\rundll32.exe[trackactivationcontextreleases]
  Queries value
                                  \label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc mage file execution} \\
options\rundll32.exe[maxdeadactivationcontexts]
  Queries value
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[globalflag]
  Queries value: HKLM\so
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[cwdillegalindllsearch]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[debugprocessheaponly]
  Queries value
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
                                  chpathmode]
options\rundll32.exe[se
                                  \label{locality} \begin{tabular}{ll} HKU\label{locality} Adefault\control\ panel\desktop[preferreduilanguages] \end{tabular}
  Queries value
  Queries value
                                  HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
                                  HKLM\software\microsoft\windows
  Queries value
nt\currentversion\compatibility32[rundll32]
  Queries value:
                                  HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value
                                  HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Oueries value
                                  HKLM\system\currentcontrolset\services\bfe[imagepath]
                                  HKLM\system\currentcontrolset\services\bfe[type]
  Queries value:
                                  HKLM\system\currentcontrolset\services\bfe[start]
HKLM\system\currentcontrolset\services\bfe[errorcontrol]
  Oueries value
  Queries value:
  Oueries value:
                                  HKLM\system\currentcontrolset\services\bfe[tag]
                                  HKLM\system\currentcontrolset\services\bfe[dependonservice]
  Queries value:
  Queries value:
                                  HKLM\system\currentcontrolset\services\bfe[dependongroup]
  Queries value:
                                  HKLM\system\currentcontrolset\services\bfe[group]
                                  HKLM\system\currentcontrolset\services\bfe[objectname]
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
  Queries value
  Oueries value:
                                  HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
  Queries value
  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
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[type]
  Queries value
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[guid]
  Oueries value
Oueries value
Queries value
HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
  Oueries value:
                                  HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
  Queries value
  Oueries value:
                                  HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
                                  HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
  Queries value
  Oueries value:
                                  HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
  Queries value:
                                  HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
  Oueries value
                                  HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
  Queries value:
                                  HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
  Oueries value
                                  Queries value:
                                  HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
  Oueries value
                                  Queries value
                                  \label{thm:local_ham} HKLM \system \current controlset \services \browser \trigger in fo \0 [data0] \\ HKLM \system \current controlset \services \browser \trigger in fo \0 [datatype1] \\
  Queries value:
  Queries value:
                                  HKLM \system \current control set \services \browser \trigger in fo \0 [data1] \\ HKLM \system \current control set \services \browser \trigger in fo \0 [datatype2] \\
  Queries value
  Queries value:
                                  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]
                                  HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
  Queries value
  Oueries value:
                                  HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
```

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]

 $\label{thm:local-problem} HKLM \system \current control set services \browser \trigger in foliaty per light control set services \browser \trigger in foliating the light control set services \browser \trigger \system \current \current$

HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]

Queries value: Oueries value:

Queries value:

Queries value

```
HKLM\svstem\currentcontrolset\services\browser\triggerinfo\1[datatype3]
     Queries value:
     Queries value
                                                                          HKLM\system\currentcontrolset\services\browser[imagepath]
                                                                          HKLM\system\currentcontrolset\services\browser[type] HKLM\system\currentcontrolset\services\browser[start]
     Oueries value:
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\browser[errorcontrol] HKLM\system\currentcontrolset\services\browser[tag]
     Queries value:
     Queries value:
                                                                          \label{thm:local_ham} HKLM \system \current controlset \services \browser[dependons ervice] \\ HKLM \system \current controlset \services \browser[dependong roup] \\
     Queries value:
     Queries value:
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\browser[group]
HKLM\system\currentcontrolset\services\browser[objectname]
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action] HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
     Oueries value
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
     Queries value
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[action]
      Queries value
     Queries 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]
                                                                          HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
     Queries value:
     Oueries value:
                                                                          HKLM\software\microsoft\sqmclient\windows[studyid]
                                                                          HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
     Queries value:
     Oueries value
HKLM \setminus system \setminus current control set \setminus services \setminus device associations ervice \setminus trigger info \setminus 0 [action]
     Oueries value
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]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype1]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[action]
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[type]
     Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[guid]
     Oueries value
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ HKLM \end{tabular} $$ is a solution service \end{tabular} $$ to solution service \end{tabular} $$ is a solution service \end{t
     Queries value
\label{local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ HKLM \end{tabular} $$ excited the local control of 
     Queries value
\label{local-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operat
     Queries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[action]
                                                                          HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[type]
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[guid]
     Queries value
     Oueries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype0]
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]
     Oueries value
                                                                          HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[guid]
     Queries value:
     Queries value
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype0]
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[data0]
     Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype1]
                                                                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
     Queries value:
     Oueries value:
                                                                          HKLM\svstem\currentcontrolset\services\dnscache\triggerinfo\0[tvpe]
                                                                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
     Queries value:
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
     Queries value:
                                                                          HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus trigger info \setminus 0 \ [data 0]
     Oueries value:
                                                                          HKLM \ system \ current control set \ services \ dns cache \ trigger in fo \ \ 0 \ [data type 1] \\ HKLM \ system \ current control set \ services \ dns cache \ [image path]
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\dnscache[type]
HKLM\system\currentcontrolset\services\dnscache[start]
     Oueries value:
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
HKLM\system\currentcontrolset\services\dnscache[tag]
     Queries value
     Queries value
                                                                          \label{thm:local-problem} HKLM \system \current controlset \services \dnscache[dependonservice] \\ HKLM \system \current controlset \services \dnscache[dependongroup]]
     Queries value:
     Queries value:
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\dnscache[group]
HKLM\system\currentcontrolset\services\dnscache[objectname]
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[action]
     Queries value
     Oueries value:
                                                                          HKLM\svstem\currentcontrolset\services\dsmsvc\triggerinfo\0[type]
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[guid]
     Queries value
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype0]
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data0]
     Queries value:
     Oueries value
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype1]
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data1]
                                                                          HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype2] HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data2]
     Oueries value:
     Queries value:
     Queries value:
Queries value:
                                                                          \label{thm:local-problem} HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype3]$ HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]$
                                                                          \label{thm:local_ham} HKLM \system \current controls et \services \efs \trigger in fool[type] \\ HKLM \system \current \controls et \services \efs \trigger in fool[guid] \\
     Queries value:
     Queries value:
                                                                          \label{thm:local-hklm} HKLM \system \current controlset \services \efs \trigger info \0 \[attype0] \ HKLM \system \current controlset \services \floor \fl
     Queries value
     Queries value:
                                                                          HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[guid]
     Queries value:
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[action]
HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[action]
     Queries value
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[type]
     Queries value
     Oueries value:
                                                                          HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[guid]
                                                                          HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[datatype0]
     Queries value:
                                                                          HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} System \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} System \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \label{lklm}
     Oueries value:
     Queries value:
     Oueries value
                                                                          HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[guid]
```

HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype0]

Queries value

```
HKLM\svstem\currentcontrolset\services\gpsvc\triggerinfo\0[data0]
  Queries value:
                               HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype1]
  Queries value
                               HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
  Oueries value:
  Queries value:
                               \label{thm:local_HKLM} HKLM \system \current controlset \services \hidserv \trigger in fo \0 [guid] \\ HKLM \system \current controlset \services \hidserv \trigger in fo \0 [data type 0] \\
  Queries value:
  Queries value:
  Queries value:
Queries value:
                               \label{thm:local-hklm} HKLM \system \current controlset \services \hidserv \trigger in fo \0 \[data0] \ HKLM \system \current controlset \services \hidserv \trigger \[datatype1] \
  Queries value
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[data0]
\label{local-problem} HKLM\system\currentcontrolset\services\homegroup provider\triggerinfo\0[datatype1] \\ Queries\value: HKLM\system\currentcontrolset\services\triggerinfo\0[action] \\
  Oueries value:
                               HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
                               HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
  Queries value:
  Oueries value:
                               HKLM \verb|\system| current control set \verb|\services| ikeext \verb|\triggerinfo| 0 [data type 0]
  Queries value:
                               HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
                               HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
HKLM\system\currentcontrolset\services\ikeext[imagepath]
  Oueries value:
  Queries value:
                               HKLM\system\currentcontrolset\services\ikeext[type] HKLM\system\currentcontrolset\services\ikeext[start]
  Oueries value:
  Queries value:
  Oueries value
                               HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
  Queries value:
                               HKLM\system\currentcontrolset\services\ikeext[tag]
                               HKLM\system\currentcontrolset\services\ikeext[dependonservice]
  Queries value
  Queries value:
                               HKLM\system\currentcontrolset\services\ikeext[dependongroup]
  Queries value
                               HKLM\system\currentcontrolset\services\ikeext[group]
  Queries value:
                               HKLM\system\currentcontrolset\services\ikeext[objectname]
  Queries value
                               HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[action]
  Oueries value:
                               \label{thm:local_ham} HKLM \system \current control set \services \key is o'trigger in fo' \label{thm:local_ham} \end{tabular} HKLM \system \current control set \services \key is o'trigger in fo' \label{thm:local_ham} \end{tabular}
  Queries value
                               HKLM \system \current control set \services \key is o \trigger in fo \0 [datatype0] \\ HKLM \system \current control set \services \key is o \trigger in fo \0 [data0] \\
  Oueries value:
  Queries value:
                               Oueries value
  Queries value:
                               HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
  Oueries value:
  Queries value:
  Queries value:
                               HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0] HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
  Queries value:
  Oueries value
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
  Queries value:
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
  Queries value
                               Queries value:
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
  Queries value
  Oueries value:
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
  Queries value
  Oueries value:
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[action]
  Queries value:
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[type]
  Oueries value:
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[guid]
                               HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[datatype0]
  Queries value:
  Queries value
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[type]
  Queries value:
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[datatype0]
  Oueries value
  Queries value:
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[action] HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[type]
  Queries value:
  Queries value:
  Queries value:
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[guid]
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[datatype0]
  Queries value:
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[action]
HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[type]
  Queries value
  Oueries value:
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[guid]
  Queries value
  Oueries value
                               HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2ſdatatype01
  Queries value
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[action]
                               HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[type]
  Queries value:
  Oueries value:
                               HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[guid]
  Queries value:
\label{local-problem} HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype0] \\ Queries\ value: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[data0] \\
  Oueries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype1]
  Queries value:
Queries value:
                               HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action] HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
  Queries value
                               HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
  Queries value
HKLM \verb|\system| current controlset \verb|\services| policy agent \verb|\triggerinfo| 0 [data type 0] |
                               Oueries value:
  Queries value
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
                               HKLM\system\currentcontrolset\services\policyagent[imagepath]
  Queries value:
  Oueries value:
                               HKLM\system\currentcontrolset\services\policyagent[type]
                               HKLM\system\currentcontrolset\services\policyagent[start]
  Queries value:
                               \label{thm:local_hammon} HKLM \system \current controls et\services \policy agent [error control] \\ HKLM \system \current controls et\services \policy agent [tag]
  Oueries value:
  Queries value:
                               HKLM\system\currentcontrolset\services\policyagent[dependonservice]
HKLM\system\currentcontrolset\services\policyagent[dependongroup]
  Oueries value:
  Queries value:
  Queries value:
Queries value:
                               HKLM\system\currentcontrolset\services\policyagent[group]
HKLM\system\currentcontrolset\services\policyagent[objectname]
  Queries value
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\remoteregistrv\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[data0]
  Queries value:
Queries value:
                               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[action]
  Oueries value:
                               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[type]
  Queries value
                               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[guid]
```

```
Queries value
                                                                            HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[action]
                                                                           HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[type] HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[guid]
     Oueries value:
     Queries value:
                                                                           Queries value:
     Queries value:
                                                                           HKLM \system \current control set \services \scards vn \trigger info \cite{thmost} if data type 1] HKLM \system \current control set \services \sens \system \current control set \services \sens \system \current \cite{thmost} if data \system \system \system \cite{thmost} if data \system \syst
     Queries value:
     Queries value:
     Oueries value:
                                                                           HKLM \setminus system \setminus current control set \setminus services \setminus sens rsvc \setminus trigger info \setminus 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]
                                                                           HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[guid]
     Queries value:
                                                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[datatype0]
      Queries value
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[action]
     Queries value
                                                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[type]
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[guid]
                                                                            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[datatype0]
     Queries value
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[action] HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[type]
     Queries value:
                                                                           \label{thm:local_ham} HKLM \system \current control set \services \sprsvc\trigger in fo \0 [guid] \\ HKLM \system \current control set \services \sprsvc\trigger in fo \0 [data type 0] \\
     Oueries value:
     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]
     Oueries value:
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[action] HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[type]
     Oueries value:
     Queries value:
     Oueries value
                                                                           HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[guid]
                                                                           HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype0]
     Queries value:
                                                                            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[data0]
      Queries value
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype1]
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[type]
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[guid]
     Queries value
HKLM \simeq control set \simeq control
     Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[data0]
     Queries value
\label{local-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operator-operat
     Queries value
\label{localization} HKLM \xspace{$\tt KLM} \xspace \xspace{\tt KLM} \xspace \xspace{\tt KLM} \xspace \xspace{\tt KLM} \xspace{\tt KLM
     Queries value
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[type]
     Queries value
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[guid]
     Oueries value
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[datatype0]
     Oueries value
Oueries value
Oueries value
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
     Oueries value
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
     Queries value
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0fdata11
     Queries value
HKLM\system\currentcontrolset\service\tabletinputservice\triggerinfo\0[datatype2]
     Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
     Queries value
HKLM\system\currentcontrolset\service\tabletinputservice\triggerinfo\0[datatype3]
     Oueries value
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} which is a property of the local partial partia
     Queries value
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[action]
     Queries value:
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[guid]
     Oueries value:
     Queries value
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[datatype0]
                                                                           HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[data0]
     Queries value:
     Oueries value:
HKLM \verb|\system| current controlset \verb|\services| time broker \verb|\triggerinfo| 0 [data type 1]
     Oueries value:
                                                                           HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[action]
     Queries value:
                                                                           HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[type]
     Oueries value:
                                                                           HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[guid]
     Queries value:
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[data0]
     Queries 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[guid]
     Oueries value:
     Queries value
HKLM\svstem\currentcontrolset\services\vmicheartbeat\triggerinfo\0[datatvpe0]
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[action]
     Queries value:
```

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

HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[guid]

Queries value

Queries value

HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[datatype0]

Queries value:

```
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[datatype0]
                                              HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[action]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[type]
                                               HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[guid]
   Queries value:
   Queries value:
                                              HKLM \verb|\system| current controlset \verb|\services| \verb|\wmicrdv| trigger in fo \verb|\o| [data type 0] |
   Queries value:
\label{local_HKLM} HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[action] \\ Queries\value: HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[type] \\
   Queries value:
   Oueries value:
                                              HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[guid]
   Queries value
Queries value:
\label{local_hammon_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[action] \end{tabular}
                                              HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[type]
   Queries value:
                                              HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[guid]
   Queries value:
\label{local_ham} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[datatype0] \end{tabular}
                                              HKLM \system \current control set \services \vmic vss \trigger in fo \0 [action] \\ HKLM \system \current control set \services \vmic vss \trigger in fo \0 [type] \\
   Queries value:
   Queries value:
   Queries value:
                                              \label{local-hklm} $HKLM \simeq \sum_{i=1}^{KLM} system \cap set services \sim injective system of the services of the ser
   Queries value:
   Oueries value:
                                              HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
                                               HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
   Queries value:
   Oueries value:
                                              HKLM \verb|\system| current controlset \verb|\services| \verb|\w32time| trigger in fo \verb|\o| [guid]|
   Queries value:
                                               HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
                                              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action] HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[action] HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[type]
   Oueries value
   Queries value:
                                               HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[guid]
    Queries value
                                              HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[datatype0]
   Queries value:
   Queries value
                                               HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[data0]
   Queries value:
                                              HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[datatype1]
   Queries value:
                                               HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
   Oueries value:
                                              HKLM\svstem\currentcontrolset\services\webclient\triggerinfo\0[tvpe]
                                               HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
   Queries value
   Oueries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
                                              \label{thm:local-problem} HKLM \system \current controls et\services \wersvc\trigger info\0 [type] \\ HKLM \system \current controls et\services \wersvc\trigger info\0 [type] \\
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
   Oueries value:
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[action] HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[type]
   Queries value:
                                              HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[guid] HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[datatype0]
   Oueries value:
   Queries value:
   Queries value:
                                               HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[data0]
   Queries value:
                                              HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[datatype1]
                                              HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[action]
HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[type]
   Queries value
   Oueries value:
                                               HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[guid]
   Queries value
   Oueries value:
                                              HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[datatype0]
   Queries value:
                                               HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[data0]
   Oueries value:
                                              Queries value:
                                              \label{thm:local} HKLM \system \current control set \services \wpdbusenum \triggerinfo \cite{thm:local} like \cite{thm:local} like
   Queries value
   Queries value:
   Oueries value
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action] HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
   Queries value:
   Queries value:
    Queries value:
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
   Queries value:
HKLM\system\currentcontrolset\services\wodbusenum\triggerinfo\2[action]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\wodbusenum\triggerinfo\2[guid]
   Queries value:
HKLM\svstem\currentcontrolset\services\wpdbusenum\triggerinfo\2\datatvpe01
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
   Queries value:
   Oueries value:
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
   Queries value:
                                               Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[action] HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[type]
   Oueries value:
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[guid]
   Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype0]
                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[data0]
   Queries value:
   Queries value
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4\datatype11
   Queries value:
                                              HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[action]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[type]
                                              HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[guid]
   Queries value
   Oueries value:
HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[datatype0]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[action]
   Queries value:
                                               HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[type]
                                              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[datatype0]
   Oueries value:
   Queries value:
   Queries value:
Queries value:
                                              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[action] HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[type]
                                              \label{thm:hklm} HKLM \system \current control set \services \wu auserv \trigger in fo \1 [guid] \\ HKLM \system \current control set \services \wu auserv \trigger in fo \1 [data type 0] \\
   Queries value:
   Queries value:
                                              HKLM \system \current control set \services \swudfsvc\trigger info\0[action] \label{eq:hklm} HKLM \system \current control set \services \swudfsvc\trigger info\0[type] \label{eq:hklm}
   Queries value
   Queries value:
                                              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
   Queries value:
   Oueries value:
   Queries value
                                               HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
                                               HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}[]
   Queries value:
   Oueries value
                                              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
                                           ver32[inprocserver32]
e212013ea917}\inprocser
   Queries value:
                                              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprocserver32[]
   Queries value
                                              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]
```

```
a5c5bc1c2ae6}\inprocserver32[inprocserver32]
     Queries value:
                                                                  HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[]
                                                                  HKCR\clsid\{c90250f3-4d7d-4991-9b69-
     Oueries value
 a5c5bc1c2ae6}\inprocserver32[threadingmodel]
     Queries value:
                                                                  HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
     Oueries value:
                                                                  HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
     Queries value:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues[capabilities]
     Queries value:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues[configflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
     Queries value:
                                                                  HKCU\control panel\desktop[caretwidth]
                                                                  HKCU\control panel\desktop[cursorblinkrate]
     Queries value:
     Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[alwaysshowmenus]
     Queries value:
 \label{thm:local_explorer_lad_vanced} HKLM \software \mbox{\sc windows \current version \explorer \advanced [always show menus]} \\
     Queries value:
                                                                  \label{thm:local-continuous} HKCU \software \microsoft \ internet explorer \toolbar [menuuser expanded] \\ HKCR \clsid \ \{f5a8b627-4d46-4d65-92f3-73626ae31971\}[]
     Oueries value:
     Oueries value
                                                                  HKCR\clsid\{f5a8b627-4d46-4d65-92f3-
 73626ae31971}\inprocserver32[inprocserver32]
                                                                  HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprocserver32[]
     Oueries value:
     Queries value
                                                                  HKCR\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprocserver32[threadingmodel]
     Queries value
Queries value
Queries value
HKL\\ M\ software \ microsoft\ windows\ current version \ explorer\ command store \ shell\ windows\ status bar [folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handler] \ described by the status bar \ folder handle
     Queries value
\label{thm:main} HKL\ M\ software \ microsoft\ windows \ current version \ (explorer\ command store\ shell\ windows\ status bar\ [invokecommand on selection]
     Oueries value
HKL^{M} software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\commandstore| shell| windows .statusbar[sendtoverb] | the status of th
     Oueries value
 HKLM\software\microsoft\windows\currentversion\explore\commandstore\shell\windows.statusbar[opencontrolpanel]
     Oueries value
\label{thm:local_hammon_hammon} HKLM \software \microsoft \windows \current version \end{tabular} explorer \command store \shell \windows . status bar[open control panel page] \end{tabular}
     Oueries value
\label{thm:hklm:hklk} HKL\@M\coftware\microsoft\windows\currentversion\explorer\commandstore\shell\windows\currentversible\property]{ }
     Queries value
\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+advanced\+[showstatusbar]
     Queries value:
                                                                  HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}[]
HKCR\clsid\{b77b1cbf-e827-44a9-a33a-
     Queries value
6ccfeeaa142a}\inprocserver32[inprocserver32]
                                                                  HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprocserver32[]
     Queries value:
     Queries value
                                                                  HKCR\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprocserver32[threadingmodel]
                                                                  HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]
     Queries value:
                                                                  HKCR\clsid\{76765b11-3f95-4af2-ac9d-
     Oueries value
 ea55d8994f1a}\inprocserver32[inprocserver32]
    Oueries value
                                                                  HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}[capabilities]
     Oueries value
                                                                  HKLM \ system \ current controls et \ enum \ swd \ printenum \ \{af 023001-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-4934-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b1-494-e0b
b8e8-d92d736469be}[configflags]
                                                                  HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[]
     Oueries value:
                                                                  HKCR\clsid\{76765b11-3f95-4af2-ac9d-
     Queries value
ea55d8994f1a}\inprocserver32[threadingmodel]

Queries value: HKLM\system\currentcontrol\set\control\devicecontainers\\623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en-us]
Queries value: HKLM\system\currentcontrol\set\control\devicecontainers\\623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en]
                                                                  HKCR\clsid\{031e4825-7b94-4dc3-b131-
     Queries value
e946b44c8dd5}[system.proplist.statusbar]
                                                                  HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
     Oueries value
11e3-be67-0800272f6e60\} \\ properties \\ \{3464f7a4-2444-40b1-980a-e0903cb6d912\} \\ \setminus 000a[]
     Oueries value:
                                                                  HKCU\control panel\desktop[smoothscroll1
     Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
     Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [list viewalphase lect]
     Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
     Queries value:
                                                                  HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}[capabilities]
     Queries value
                                                                  HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}[]
     Queries value:
Queries value: HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-b8e8-d92d736469be}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011[]
                                                                  HKLM\system\currentcontrolset\control\devicecontainers\\{623cc955-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en-us]
                                                                  HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
     Queries value:
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en]
                                                                  HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
     Queries value:
     Oueries value
                                                                  HKCR\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprocserver32[inprocserver32]
     Oueries value
                                                                  HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprocserver32[]
                                                                  HKLM\system\currentcontrolset\control\devicecontainers\\\ 623cc955-8780-
     Queries value
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[]
Queries value: HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011[]
Queries value
HKLM \setminus system \setminus current control set \setminus control \setminus graphics drivers \setminus configuration \setminus msbdd\_noedid\_1414\_008d\_ffffffff\_0 \cap cc77560 bc3634a486857716562968286[setid]
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\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\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
     Oueries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00ab02a9ab10912b3b7f8c017a344c8d14[setid]
     Oueries value
 Oueries value:
\label{thm:hklmsystem} HKLM\system \\ \controlset\\ \cont
     Queries value:
```

Queries value:

HKCR\clsid\{c90250f3-4d7d-4991-9b69-

```
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0 00 07db c6^182fdc0875f0a76803e4a9848a8c1ea7ftimestamol
                                                                                                       HKCR\clsid\{21ec2020-3aea-1069-a2dd
08002b30309d}\shellfolder[attributes]
                                                                                                       HKCR\clsid\{21ec2020-3aea-1069-a2dd-
       Queries value
08002b30309d}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[foldervalueflags]
Queries value: HKCR\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprocserver32[threadingmodel]
       Queries value
Queries value
Queries value
HKLM \setminus system \setminus current control \setminus graphics drivers \setminus configuration \setminus msbdd\_noedid\_80ee\_beef\_00000000\_00020000\_0^ab02a9ab10912b3b7f8c017a344c8d14 \setminus 00[stride]
       Oueries value
HKLM \system \current control set \control \system \current control \system \current \control \system \current \cu
      Oueries value
Oueries value
Oueries value
\label{thm:local_hammon_hammon} HKLM \software \mbox{$\mbox{$\mbox{$w$indows$} \currentversion$} policies \nonenum[{21ec2020-3aea-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-a2dd-1069
08002b30309d}1
       Queries value:
                                                                                                       HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}[sortorderindex]
        Oueries value:
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 00ab02a9ab10912b3b7f8c017a344c8d14\00[position.cy]
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[flags]
HKLM\system\currentcontrol\set\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[videostandard]
HKLM \system \current control \system \current control \system \current control \system \current \current \system \current \current \system \current \current \system \current \system \current \current \system \current \system \current \system \current \system \system \current \system \system \current \system \syste
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[activesize.cv]
       Queries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[vsvncfreq.numerator]
       Queries value
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00fvsyncfreq.denominatorl
       Queries value:
HKLM \system \current control \system \current control \system \current control \system \current \current \system \current \current \system \current \system \current \system \current \system \syst
       Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_0020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[hsyncfreq.denominator]

Queries value: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[system.statusicons]
        Oueries value
                                                                                                       HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{7a55582b-bd8c-4475-
b94c-b87a388a7899} 100]
                                                                                                       HKCR\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}[system.librarylocationscount]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[pixelrate]
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0020000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00fscanlineordering]
HKLM \system \current control \system \current control \system \current control \system \current \current \system \current \current \system \current \current \system \current \system \system \current \system \sys
       Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd noedid 80ee beef 00000000 0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[rotation]
                                                                                                       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:
       Oueries value:
                                                                                                       b8c8-bd6624e1d032} 251
HKLM\software\microsoft\windows\currentversion\policies\explorer[notaskgrouping]
       Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbarglomlevel]
       Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbaranimations]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbarsmallicons]
       Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[taskbarsmallicons]
       Queries value:
HKLM \label{lem:hklm} Which is a constant with the statement of the stat
       Queries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ my computer \ names pace \ delegate folders \ []
       Queries value:
Queries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ my computer \ names pace \ delegate folders \ \{35786d3c-market \ names 
b075-49b9-88dd-029876e11c01}[suppressionpolicy]
       Oueries value:
HKLM \label{eq:hkkkk} In the latest and the lates
00a3-46b9-bc5f-9c04daddd5d7}[suppressionpolicy]
       Queries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ my computer \ names pace \ delegate folders \ \{b155bdf8-microsoft\ my computer \ names pace \ delegate folders \ \{b155bdf8-microsoft\ my computer \ names pace \ delegate folders \ \{b155bdf8-microsoft\ my computer \ names pace \ delegate folders \ folders \ names 
02f0-451e-9a26-ae317cfd7779}[suppressionpolicy]
       Oueries value:
 HKCU \setminus software \\ \mbox{microsoft} \\ \mbox{windows} \\ \mbox{currentversion} \\ \mbox{explorer} \\ \mbox{mountpoints2} \\ \mbox{cpc} \\ \mbox{volume} \\ \mbox{d5291c64-7c88-1000} \\ \mbox{d5291c64-7c88-1
11e3-be65-806e6f6e6963}[generation]
       Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders[suppressionpolicy]
       Queries value
HKLM \label{limits} In the limits of the l
       Oueries value:
HKLMNs of tware \mbox{\tt libraries} names pace \mbox{\tt delegate folders} \{896664f7-12e1-490f-8782-c0835 afd 98fc} [suppression policy]
                                                                                                      HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[sortorderindex]
HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Queries value:
       Oueries value
8d23b85255bf}\shellfolder[attributes]
                                                                                                      HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value
8d23b85255bf}\shellfolder[callforattributes]
       Oueries value
                                                                                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[restrictedattributes]
      Oueries value
                                                                                                      HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[foldervalueflags]
                                                                                                       HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
       Oueries value
```

8d23b85255bf}\shellfolder[wantsfordisplay]

```
Queries value
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[hidefolderverbs]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
   Oueries value
 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]
    Oueries value
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[queryforoverlay]
Queries value: HKCR\clsid\\9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[mapnetdriveverbs]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
    Queries valu
8d23b85255bf}\shellfolder[queryforinfotip]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[hideinwebview]
                                                         HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
Queries value: Inscring Transcript | Control of the Control of the
8d23b85255bf}\shellfolder[wantsaliasednotifications]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
Queries value: HKCR\clsid\\9c73f5e5-7ae 8d23b85255bf}\shellfolder[wantsuniversaldelegate]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
    Queries value:
Queries value: hKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[hasnavigationenum]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
Queries value: INGCCC1sid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[nodefaulttofs]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
    Queries value
8d23b85255bf}\shellfolder[parsedisplaynameneedsurl]
    Oueries value
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[blocknewfile]
    Oueries value
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[noinitrequired]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
    Oueries value
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 valu
                                                        HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf} {000214e6-0000-0000-c000-000000000046}}
 0xffff]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[]
    Queries value
Queries value: HKCR\clsid\{9c73f5e
8d23b85255bf}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
    Queries value
                                                        HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.namespaceclsid]
    Oueries value
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2-
b5d6-00c04fd918d0} 61
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}[system.ispinnedtonamespacetree]
    Oueries value
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{5d76b67f-9b3d-44bb-
b6ae-25da4f638a67} 2]
    Queries value:
                                                        HKCR \verb|\clsid|{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.hideondesktop]| \\
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2-
    Queries value
b5d6-00c04fd918d0} 341
                                                        HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
    Queries value:
3aea-1069-a2d8-08002b30309d}\defaulticon[]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\defaulticon[openicon]
    Oueries value:
 HKLM \label{lem:hklm} Which is the latest and the
3aea-1069-a2d8-08002b30309d}1
Queries value: HKCU\.
3aea-1069-a2d8-08002b30309d}[]
                                                        HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
    Queries value:
                                                        HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localized string]
    Oueries value:
                                                        \label{thm:hammon} HKLM \system \current controls et\services \dcomlaunch \figure{1}{0} bject name \figure{1}{1}{1} HKLM \system \current \controls et\services \system \figure{1}{1}{1}{1} bject \current \controls et\services \system \figure{1}{1}{1}{1} bject \current \cu
    Queries value:
                                                        HKLM\system\currentcontrolset\services\rpcss[objectname]
HKLM\system\currentcontrolset\services\eventsystem[objectname]
    Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\services\bits[objectname] HKLM\system\currentcontrolset\services\bits[imagepath]
    Oueries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\services\bits[wow64]
HKLM\system\currentcontrolset\services\bits[requiredprivileges]
    Queries value:
    Queries value:
    Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
                                                        HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}[]
    Queries value:
                                                        HKCR\clsid\{603d3801-bd81-11d0-a3a5-
    Oueries value:
00c04fd706ec}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[]
    Oueries value:
    Queries value:
                                                        HKCR\clsid\{603d3801-bd81-11d0-a3a5-
Queries value:
Queries value:
                                                        HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
                                                        HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}[]
                                                        Queries value
 79ce68d8abc2}\inprocserver32finprocserver321
    Queries value:
                                                        HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32[]
                                                        HKCR\clsid\{317d06e8-5f24-433d-bdf7-
    Oueries value:
 79ce68d8abc2}\inprocserver32[threadingmodel]
                                                        HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}[]
    Oueries value:
                                                        HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-
    Queries value:
850b2087f5dd}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32[]
    Queries value:
    Queries value
                                                        HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprocserver32[threadingmodel]
```

```
Queries value:
HKL^{M} \ software \ microsoft \ windows \ current version \ photoproperty handler \ container associations \ [\{57a37caa-mainer associations, and the container association of the container as th
367a-4540-916b-f183c5093a4b}1
                                                        HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]
   Queries value:
   Queries value:
                                                        HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32[inprocserver32]
   Queries value:
Queries value:
                                                        323e85a1ce84}\inprocserver32[threadingmodel]
                                                        HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-
   Queries value:
8539-9230a44081a51
                                                        HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-
   Queries value
809b-2a87b70881f8]
                                                        HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-
   Queries value:
833b-323e85a1ce84]
                                                        HKLM\software\policies\microsoft\internet
   Queries value
explorer\security[disablesecuritysettingscheck]
   Queries value
                                                        HKLM\software\policies\microsoft\internet
explorer\security[disabl
                                                      lefixsecuritysettings]
   Oueries value:
                                                        HKCU\software\microsoft\internet
explorer\security[disablefixsecuritysettings]
                                                        HKLM\software\microsoft\internet
   .
Oueries value
explorer\security[disablefixsecuritysettings]
   Oueries 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]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102[checksetting]
                                                        HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837\}.check.104[checksetting]
                                                        HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]

HKCR\clsid\{ca236752-2e77-4386-b63b-
   Queries value:
   Oueries value
0e34774a413d}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[1
   Oueries value:
   Queries value
                                                        HKCR\clsid\{ca236752-2e77-4386-b63b-
\label{lem:condition} Oe34774a413d\\ \mbox{ \begin{tabular}{ll} \label{lem:condition} \mbox{ \end{tabular} } WLM\software\mbox{ \begin{tabular}{ll} \mbox{ 
   Queries value
                                                        9270-3b2691a0a394]
Queries value:
86ba-948b70416220]
                                                        HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-
                                                        \label{thm:loss} HKLM\software\microsoft\windows\windows\ error\ reporting[disabled] HKCU\software\microsoft\windows\windows\ error\ reporting[disabled] \\
   Queries 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-
   Oueries value
0040963251e5}\inprocser
                                                       er32[inprocserver32]
                                                        HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]
   Oueries value:
                                                         HKCR\clsid\{88d96a05-f192-11d4-a65f
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
                                                        HKCU\software\microsoft\windows\windows error
   Queries value:
reporting[lastqueuepestertime]
                                                        HKLM\software\microsoft\windows\windows error
   Queries value:
reporting[queuepesterinterval]
                                                        HKCU\software\microsoft\windows\windows error
   Queries value:
reporting[queuepesterinterval]
                                                        HKCU\software\microsoft\windows\currentversion\action
   Queries value:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\}.check.101[checksetting]
Queries value: HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4\}[]
   Queries value:
                                                        HKCR\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
   Queries value:
   Oueries value
                                                        HKCR\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32[threadingmodel]
   Oueries value
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \microsoft \windows \current version \policies \system [enable lua] \end{tabular}
Queries\ value: \\ HKCU\software\mbox{\mbox{microsoft}\windows\currentversion\action} center\checks\cee6f269-b90a-4053-a3be-499afcec98c4\}.check.0[checksetting]
   Queries value:
                                                        HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}[]
                                                        HKCR\clsid\{088e8dfb-2464-4c21-bad2-
   Queries value
f0aa6db5d4bc}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
                                                        \label{local-equation} HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[]$ HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0a6db5d4bc}\
    Queries value:
   Queries value
f0aa6db5d4bc}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[inprocserver32]
                                                        HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
   Oueries value:
                                                        HKLM\software\policies\microsoft\windows\system[enablesmartscreen]
    Queries value:
   Oueries value
                                                        HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[threadingmodel]
   Oueries value
HKLM\software\microsoft\windows\currentversion\explorer[smartscreenenabled]
   Oueries value
                                                        HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
   Queries value:
Queries value:
                                                        \label{local-equation} HKCR\interface \ \{b722bccb-4e68-101b-a2bc-00aa00404770\}\ proxystubclsid32[]\\ HKCR\clsid \ \{d26de5c1-c061-43f7-9c40-7517526cf1c1\}[]
   Queries value:
                                                        HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
                                                        HKCR\clsid\{d26de5c1-c061-43f7-9c40-
   Queries value
7517526cf1c1}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[]
   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-
   Oueries value
e4fddd701cba}\inprocserver32[threadingmodel]
                                                        HKCR\clsid\{d26de5c1-c061-43f7-9c40-
   Oueries value
7517526cf1c1}\inprocserver32[threadingmodel]
   Oueries value
\label{thm:linear} \parbox{$HKCU$\software\mbox{$microsoft\windows\currentversion\startupnotify[enablestartupappnotification]}} \parbox{$HKCU$\software\mbox{$microsoft\windows\currentversion\startupnotify[enablestartupappnotification]}} \parbox{$HKCU$\software\mbox{$microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]}} \parbox{$HKCU$\software\mbox{$microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]}} \parbox{$Microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]} \parbox{$Microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]} \parbox{$Microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]} \parbox{$Microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]} \parbox{$Microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]} \parbox{$Microsoft\windows\currentversion\startupnotify[enablestartupappnotification]]} \parbox{$Microsoft\windows\currentversion\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotification\startupnotificati
   Oueries value
                                                        HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting]
```

```
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
                                            HKCU\software\microsoft\windows\currentversion\action
42fa-414c-b8aa-eee2c8202018}.check.100[checksetting]
   Queries value
center\checks\{01979c6a
                                           HKCU\software\microsoft\windows\currentversion\action 42fa-414c-b8aa-eee2c8202018}.check.101[checksetting]
   Queries value
center\checks\{01979c6a-
\label{lem:queries} Queries \ value: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881\}[lastknownstate]}
   Oueries 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]
Queries value: HKCU\software\microsoft\windows\currentversion\action center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101[checksetting]
                                             HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate]
                                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100[checksetting]
                                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017\}.check.800[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center \providers \end{align*} \end{align*} center \providers \end{align*} \end{align*} \end{align*} \end{align*} align*} \end{align*} align*} \end{align*} \end{align*} \end{align*} \end{align*} \end{align*} align*} \end{align*} \end{ali
                                             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
                                eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}[lastknownstate]
center\providers\
                                             HKCU\software\microsoft\windows\currentversion\action
   Queries value
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100[checksetting]
                                             HKCU\software\microsoft\windows\currentversion\action
   Queries value
center\checks\{3ff37a1c
                                           a68d-4d6e-8c9b-f79e8b16c482}.check.100[checksetting]
  Queries value
                                             HKCU\software\microsoft\windows\currentversion\action
center\providers
                                eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}[lastknownstate]
   Oueries value
                                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100[checksetting]
   Oueries value
                                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010[checksetting]
   Oueries value
                                             HKCU\software\microsoft\windows\currentversion\action
center \providers \eventlog \aa4c798d-d91b-4b07-a013-787f5803d6fc \end{figure} [lastknown state]
                                             HKCU\software\microsoft\windows\currentversion\action
center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100[checksetting]
   Oueries value
                                             HKLM \verb|\system| current control set \verb|\services| bits[type]|
                                             HKLM\system\currentcontrolset\services\bits[start]
   Queries value:
   Queries value
                                             HKLM\system\currentcontrolset\services\bits[errorcontrol]
HKLM\system\currentcontrolset\services\bits[tag]
   Queries value:
   Oueries value
                                             HKLM\system\currentcontrolset\services\bits[dependonservice]
   Queries value:
                                             HKLM\system\currentcontrolset\services\bits[dependongroup]
                                             HKLM\system\currentcontrolset\services\bits[group]
   Queries value
   Queries value:
                                             HKLM\system\currentcontrolset\services\sppsvc[objectname]
                                             HKLM\system\currentcontrolset\services\sppsvc[imagepath]
   Queries value
   Oueries value
                                             HKLM\system\currentcontrolset\services\sppsyc[wow641
                                             HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
   Queries value
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
20[profileimagepath]
   Oueries value
                                             HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
   Oueries value
                                             HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
   Oueries value
                                             HKLM\system\currentcontrolset\services\sppsvc[environment]
                                             HKLM\system\currentcontrolset\services\sppsvc[startprotected]
   Queries value:
                                             HKLM\software\microsoft\ole[pageallocatorusesystemheap]
HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:
   Queries value:
   Queries value:
                                             HKLM\software\microsoft\ole[aggressivemtatesting]
   Queries value
                                             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[sppsvc]
                                             HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
   Oueries value
                                             HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472c-
   Queries value
a5f9-f2bdfea0f1561
   Queries value:
                                             {\tt HKLM \ } system \verb|\ current control \ \\ lsa[every one includes an ony mous]
   Oueries value:
                                             HKLM\svstem\currentcontrolset\services\http[objectname]
                                             HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
   Queries value
                                             HKLM\system\currentcontrolset\services\ssdpsrv[imagepath]
   Oueries value:
   Queries value:
                                             HKLM\system\currentcontrolset\services\ssdpsrv[wow64]
   Oueries value
                                             \label{thm:local_ham} HKLM \system \current control set \services \system \current control set \system \system \current \system \system \current \system \sy
   Queries value
nt\currentversion\softwa
                                           reprotectionplatform[inactivityshutdowndelay]
                                             HKLM\software\microsoft\windows
   Queries value
                                            reprotectionplatform[keeprunningthresholdmins]
HKLM\system\currentcontrolset\services\wsearch[objectname]
nt\currentversion\softwa
   Queries value
                                             \label{thm:local-hklm} HKLM \system \current control set \services \swmpnet works vc[object name] \\ HKLM \software \swmcrosoft \cryptography \defaults \provider \swmcrosoft \strong \\
   Queries value
   Queries value
cryptographic provider[type]
                                             HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
   Oueries value
cryptographic provider[image path]
   Oueries value
                                             HKLM\software\microsoft\windows
nt\currentversion\softwa
                                             reprotectionplatform[tokenstore]
   Oueries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1[]
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10[]
   Queries value:
   Oueries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11[]
   Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12[]
   Oueries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13[]
   Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14[]
   Queries value:
Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15[]
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16[]
   Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17[]
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18[]
   Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19[]
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2[]
   Queries value
   Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20[]
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21[]
   Queries value:
   Oueries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22[]
HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23[]
   Queries value
   Oueries 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[]
   Queries value:
   Oueries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27[]
   Queries value:
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28[]
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29[]
   Oueries value
   Queries value
                                             HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3[]
```

HKCU\software\microsoft\windows\currentversion\action

Queries value

```
Queries value
                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30[]
                                                                                  HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31[]
      Queries value
      Oueries value
                                                                                 \label{local-eq:hklm} $$HKLM \simeq \frac{1-0341-4b93-85cd-72606c2df94c-6p-32[]}{}
      Queries value:
                                                                                  HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33[]
      Queries value:
                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4[]
                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5[]
      Queries value:
                                                                                 \label{eq:hklmsystem} HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6[]\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7[]\\ HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-7[]\\ HKLM\system\
      Queries value:
      Queries value:
     Queries value
                                                                                 HKLM \ system \ wpa \ 8 dec 0 af 1 - 0341 - 4b 93 - 85 cd - 72606 c 2d f 94 c - 6p - 8[]
                                                                                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9[]
      Queries value:
     Queries value:
                                                                                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
12006ef9b32a[manifestfile]
                                                                                 HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
12006ef9b32a[pluginfile]
                                                                                 HKLM\software\microsoft\windows
nt \verb|\currentversion| software protection platform \verb|\plugins| modules \verb|\c42d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4af4-a0dd-4d83ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84ff-5958-4d84
ba02fed39662[manifestfile]
    Queries value:
                                                                                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-
ba02fed39662[pluginfile]
     Queries value:
                                                                                 HKLM\software\microsoft\windows
\label{lem:nt-current-current} $$ nt\current-version\software-protection platform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[moduleid] $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$
     Queries value:
                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
HKLM\software\microsoft\windows
nt\currentversion\softw
     Queries value
nt\currentversi
                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[isservice]
                                                                                 HKLM\software\microsoft\windows
     Queries value
nt\currentversio
                                                                                   eprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[moduleid]
     Queries value
                                                                                 HKLM\software\microsoft\windows
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[moduleid]
nt\currentversi
     Queries value
                                                                                 HKLM\software\microsoft\windows
nt\currentvers
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[moduleid]
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversio
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion\softw
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[moduleid]
     Oueries value
                                                                                 HKLM\software\microsoft\window
Oueries value
                                                                                 HKI M\software\microsoft\window
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft:rm/algorithm/vmd/1.0[moduleid]| and the properties of th
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
     Queries value
                                                                                 HKLM\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[moduleid]
                                                                                 HKLM\software\microsoft\windov
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[moduleid]
                                                                                 HKLM\software\microsoft\window
                                                            softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[moduleid]
nt\currentversion
                                                                                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[moduleid]
                                                                                 HKLM\software\microsoft\windows
     Queries value
\label{lem:nt-current-constraint-current-constraint-current-current-constraint-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-current-curre
nt\currentversi
                                                                                reprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[moduleid]
     Queries value
                                                                                 HKLM\software\microsoft\windows
                                                                                reprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[moduleid]
HKLM\software\microsoft\windows
nt\currentversio
     Queries value
nt\currentversi
                                                                                 reprotection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/payloadhandler/eul/1.0[moduleid]|
                                                                                 HKLM\software\microsoft\windows
     Queries value
nt\currentversi
                                                                                   eprotection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/payloadhandler/pa/1.0[moduleid]|
     Queries value
                                                                                 HKLM\software\microsoft\windows
nt\currentversi
                                                                                  reprotection platform \verb|\plugins| objects \verb|\msft|: spp/license acquisition/payload handler/pkc/1.0[module id]|
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversio
                                                                                 reprotection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/payloadhandler/rac/1.0[moduleid]|
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion
                                                                                 eprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[moduleid]
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion
                                                                                 reprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[moduleid]
     Oueries value
                                                                                 HKLM\software\microsoft\window
\verb| nticurrent version| software protection platform \verb| plugins| objects \verb| msft:spp/statecollector/pkey[moduleid]| | the province of the protection of the
                                                                                 HKI M\software\microsoft\windo
     Oueries value
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft|: spp/task scheduler/1.0[moduleid]| and the substitution of the 
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
                                                                               HKLM\software\microsoft\windows
ureprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[moduleid]
     Queries value
nt\currentversion
                                                                                 HKLM\software\microsoft\window
     Oueries value
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft|: spp/windows functionality/agent/7.0[moduleid]| and the province of the pro
                                                                                 HKLM\software\microsoft\windov
     Queries value
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[isservice]
     Queries value
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
     Queries value
                                                                                 HKLM\software\microsoft\windows
                                                            softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[isservice]
    HKLM\software\microsoft\windows
nt\currentversion
     Queries value
                                                            software protection platform \verb|\plugins| objects| msft:rm/algorithm/flags/1.0[isservice] \\ HKLM \verb|\software| microsoft| windows
nt\currentversion
     Queries value:
nt\currentversio
                                                                                reprotection platform \verb|\plugins\>| objects \verb|\msft:rm/algorithm/hwid/4.0[isservice]|
     Queries value:
                                                                                 HKLM\software\microsoft\windows
nt\currentversio
Queries value:
                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[isservice]
HKLM\software\microsoft\windows
nt\currentversion
                                                                               reprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[isservice]
                                                                                 HKLM\software\microsoft\windows
     Queries value
                                                                                reprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[isservice]
HKLM\software\microsoft\windows
nt\currentversion
     Queries value
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[isservice]
nt\currentversion
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversio
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[isservice]
     Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion
                                                                                 reprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[isservice]
     Oueries value
                                                                                 HKLM\software\microsoft\window
Oueries value
                                                                                 HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[isservice]
                                                                                 HKLM\software\microsoft\windov
\verb|nticurrent| version is of tware protection platform is objects in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection platform is object. It is object in the continuous of tware protection of the continuous of tware protection of tware protection of the continuous of tware protection of the continuous of tware protection of the continuous of tware protection of tware protection of the continuous of the continuous of tware protection of the continuous of the c
```

```
Queries value:
                                                                                                       HKLM\software\microsoft\windows
Queries value:
                                                                                                       HKLM\software\microsoft\windows
                                                                                                      reprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[isservice]
 nt\currentversion\softw
      Queries value
                                                                                                       HKLM\software\microsoft\windows
\verb|nticurrent| version is of twa reprotection platform in the constant of the
\label{lem:queries} Queries \ value: \ HKLM\ software \ increases ftwindows \\ nt\ current version\ software protection platform\ plugins\ objects\ msft: spp/collector/global/1.0 [isservice] \\
       Oueries value
                                                                                                       HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[isservice]
       Oueries value
                                                                                                       HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[isservice]
                                                                                                       HKLM\software\microsoft\window
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[isservice]
                                                                                                       HKLM\software\microsoft\windo
nt`current version \verb|\software| protection platform \verb|\plugins| objects \verb|\msft:spp/licenseacquisition/payloadhandler/pkc/1.0[isservice]|
                                                                                                       HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[isservice]
Queries value: HKLM\software\microsoft\windows
\label{lem:ntcurrent} $$ nt\currentversion\software protection platform\plugins\objects\msft: spp/license acquisition/payload handler/spc/1.0[isservice] $$ Queries value: $$ HKLM\software\microsoft\windows $$
Queries value: https://doi.org/10.1016/j.com/spl.gins/objects/msft:spp/licenseacquisition/sequence/1.0[isservice]
Queries value: Httm\software\microsoft\windows
nt \verb|\current version| software protection platform \verb|\plugins| objects \verb|\msft|: spp/statecollector/pkey[isservice]| and the platform of th
       Queries value:
                                                                                                       HKLM\software\microsoft\windows
\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
\verb|nt'| current version \verb|software| protection platform \verb|plugins| objects \verb|wsft:spp/volume/services| kms/1.0[isservice]| | the province of the protection of the protection
                                                                                                       HKLM\software\microsoft\windows
       Queries value:
\verb|nticurrent| version is of tware protection platform is objects in structure of the stru
                                                                                                       HKLM\software\microsoft\rpc\extensions[ndroleextdll]
       Queries value:
                                                                                                       HKLM\software\microsoft\com3[finalizeractivitybypass
         Queries value:
                                                                                                       HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
       Queries value:
        Queries value
                                                                                                       HKCU\software\microsoft\window
nt\currentversion\softwareprotectionplatform[kmshostconfig]
                                                                                                       HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[enabletestvolumeintervals]
                                                                                                       HKLM\software\microsoft\windows
       Queries value:
nt\currentversion\softwareprotectionplatform[vlactivationinterval]
       Queries value:
                                                                                                       HKLM\software\microsoft\windows
Queries value: HKLM\software\microsoft\windows

HKLM\software\microsoft\windows
\verb|nt\currentversion\software protection platform[action list]|
       Oueries value
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} in $$ \color= \co
                                                                                                       HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\softwareprotectionplatform[cachestore]
       Queries value:
                                                                                                       HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
        Queries value:
                                                                                                       HKLM\system\setup\status[auditboot]
                                                                                                       HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[hardwareid]
       Queries value:
                                                                                                       HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[compatibleids]
        Queries value:
       Oueries value
 HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00[hardwareid]
       Oueries value
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 1237&subsys 00000000&rev 02\3&267a616a&1&00[compatibleids]
Oueries value
HKL \\ M\xspace{Mk.ml.} M\xspace{Mk.ml.} MkL \\ M\xspace{Mk.ml.} MkL
       Queries value:
                                                                                                       Queries value:
\label{local_holds} \begin{tabular}{ll} HKLM \end{tabular} Ake 0.303 \end{tabular} $$ 44.0 $$ [compatible ids] $$ $$ (a) $$ (b) $$ (b) $$ (c) $$ (c
                                                                                                       HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[hardwareid]
       Queries value:
        Queries value
HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[compatibleids]
                                                                                                       HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[hardwareid]
       Oueries value
\label{local_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ HKLM \end{tabular} $$ A4480 \end{tabular} $$ a84480 \end{tabular
                                                                                                       HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0fhardwareidl
      Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[compatibleids]
       Queries value:
Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[hardwareid]
       Queries value:
        Oueries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[compatibleids]
       Queries value:
                                                                                                       HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[hardwareid]
        Queries value
Oueries value
HKL \\ M\xspace{Mk.ml.} M\xspace{Mk.ml.} MkL \\ M\xspace{Mk.ml.} MkL
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[hardwareid]
       Oueries value
\label{local_hammon_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\enum\pciide\idechannel\4\&20064fa2\&0\&0[compatibleids]] \end{tabular}
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&34baf594&0&0.0.0[compatibleids]
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[hardwareid]
       Queries value
\label{local_hammon_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\enum\pciide\idechannel\4\&20064fa2\&0\&1[compatibleids]] \end{tabular}
Quer\'{ies}\ value: \\ HKLM\software\mbox{\sc microsoft\windows} \\ nt\current\version\software\protection platform[licstatusarray] \\
                                                                                                      HKLM\software\microsoft\windows
       Queries value
nt\currentversion\softwareprotectionplatform[policyvaluesarray]
       Queries value:
                                                                                                      HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[hasooberun]
                                                                                                       HKLM\software\microsoft\com3[com+enabled]
       Queries value:
                                                                                                       HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}[]
       Oueries value:
                                                                                                       HKCR\clsid\{88d96a06-f192-11d4-a65f-
        Queries value:
0040963251e5}\inprocserver32[inprocserver32]
       Queries value:
                                                                                                       HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32[]
       Queries value
                                                                                                       HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
```

```
Queries value:
                                                                  HKLM\software\microsoft\ole[maxsxshashcount]
                                                                  HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
     Queries value
                                                                  HKCU\control panel\international[scurrencyoverride]
HKLM\software\microsoft\windows
    Queries value:
     Oueries value
nt\currentversion\softwareprotectionplatform[servicesessionid]
                                                                  HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}[]
    Queries value:
Queries value: HKCR\clsid\\ 88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32[inprocserver32]
                                                                  HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32[]
    Oueries value
                                                                  HKCR\clsid\{88d96a08-f192-11d4-a65f-
    Queries value
0040963251e5}\inprocserver32[threadingmodel]
                                                                  HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\softwareprotectionplatform[logcontext]
Queries value: HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]
                                                                  HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
     Queries value
73e6154572dd}\inprocserver32[inprocserver32]
    Queries value:
                                                                  HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
    Queries value
                                                                  HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[threadingmodel]
    Oueries value:
                                                                 \label{local-hklm-system-current} HKLM \system \current control set \control product options [product policy] \\ HKLM \software \sww6432 node \switchise microsoft \direct3d \switchise microsoft \direct3d \switchise microsoft \switchise mic
     Sets/Creates value:
    Sets/Creates value:
                                                                  HKU\.default\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
    Sets/Creates value
                                                                  HKU\.default\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[]
    Sets/Creates value:
                                                                  HKLM \ system \ wpa \ 8 dec 0 af 1 - 0341 - 4b 93 - 85 cd - 72606 c 2df 94 c - 6p - 34[]
                                                                  HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name]
     Value changes:
    Value changes:
                                                                  HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
   Value changes:
Value changes:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cdot parameters \setminus protocol\_catalog9 \setminus catalog\_entries \setminus 0000000000009[packed catalogitem]
    Value changes
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
   Value changes
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
    Value changes:
Value changes
Value changes
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000000004 \ [packed catalog item]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000003[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000002[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000001[packedcatalogitem]
    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 \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries 64 \noonumber \n
    Value changes:
HKLM \system \current controls et \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries 64 \no 00000000004 \[packed catalogitem] \label{eq:hklm}
    Value changes:
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \\64 \colonormal \parameters \protocol\_catalog9 \catalog9 
   Value changes:
HKLM \system \correct control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries 64 \colongormal to the discount of the control set \services \colongormal to the control set \colon
    Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
   Value changes
Value changes
\label{librarypath} HKLM \system \current controlset \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names \
   Value changes
Value changes:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \mid parameters \setminus names pace\_catalog 5 \setminus catalog\_entries 64 \setminus 0000000000004 \{library path\}
   Value changes:
                                                                  HKLM\system\currentcontrolset\services\browser[star
                                                                  HKLM\system\currentcontrolset\services\policyagent[start]
    Value changes:
    Value changes:
                                                                  HKCU\software\microsoft\internet
explorer\toolbar\shellbrowser[itbar7layout]
    Value changes:
                                                                  {\tt HKCU \ } software \verb|\microsoft \ windows \verb|\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]
                                                                  HKCU\software\microsoft\windows\currentversion\action
   Value changes:
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2\.check.101[checksetting]
                                                                  HKCU\software\microsoft\windows\currentversion\action
    Value changes:
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]
                                                                  HKCU\software\microsoft\windows\currentversion\action
    Value changes:
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4\}.check.0[checksetting]
```

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