# Malware Analysis Appliance by Blue Coat Systems, Inc.

# Task Details

Task ID: Risk Level:

Date Processed: 2016-04-07 08:21:32 (UTC) Processing Time 61.23 seconds

Virtual Environment: IntelliVM

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

Sample ID Type: basic Owner: admir

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

File Type: PE32:win32 File Size: 10254 bytes

MD5 1439e0552127dda0c66b7be1eadb723d

SHA256: 89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a

Description:

# Pattern Matching Results

Modifies registry autorun entrie Writes to system32 folder

3 Program causes a crash [Info]
5 Installs service

PE: File has TLS callbacks

PE: Nonstandard section

3 Writes to a log file [Info]

4 Terminates process under Windows subfolder
4 Connects to local IP

3 Long sleep detected 2 Resolves local hostname

#### Static Events

Anomaly Contains a virtual section

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

### Process/Thread Events

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

["C:\windows\temp\ToggleService32.exe" ]
Creates process: C:\windows\System32\alg.exe [C:\windows\System32\alg.exe] Creates process: Creates process: C:\Windows\System32\msdtc.exe [C:\Windows\System32\msdtc.exe]
C:\Windows\system32\UIODetect.exe [C:\Windows\system32\UIODetect.exe] Creates process: C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe -

LocalServicePeerNet]

C:\Windows\System32\spoolsv.exe [C:\Windows\System32\spoolsv.exe] Creates process: Creates process: Creates process: C:\Windows\system32\vssvc.exe [C:\Windows\system32\vssvc.exe]
C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe WerSvcGroup]

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

imgsvc]

Loads service: ALG [C:\Windows\System32\alg.exe]
AppMgmt [C:\Windows\system32\svchost.exe -k netsvcs]

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

TrkWks [C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted]
MSDTC [C:\Windows\System32\msdtc.exe] Loads service:

Loads service:

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

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

Loads service

Loads service: Loads service: Spooler [C:\Windows\System32\spoolsv.exe]
RpcSs [C:\Windows\system32\svchost.exe -k rpcss]
SecLogon [C:\Windows\system32\svchost.exe -k netsvcs] Loads service: SENS [C:\Windows\system32\svchost.exe -k netsvcs]
SysMain [C:\Windows\system32\svchost.exe -k Loads service: Loads service:

LocalSystemNetworkRestricted]
Loads service: Sche

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

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

VSS [C:\Windows\system32\vssvc.exe] Loads service:

Loads service: Audio:
LocalServiceNetworkRestricted] AudioSrv [C:\Windows\System32\svchost.exe -k

Loads service: WERSvc [C:\Windows\System32\sychost.exe -k WerSvcGroup] Loads service:

WEASYC [C::Windows\system32\svchost.exe - ke1s\csioupj]
MpsSvc [C::Windows\system32\svchost.exe - k LocalServiceNoNetwork]
STISvc [C::Windows\system32\svchost.exe - k imgsvc] Loads service: Loads service: Loads service: W32Time [C:\Windows\system32\svchost.exe -k LocalService] WUAUServ [C:\Windows\system32\svchost.exe -k netsvcs]

Loads service:  $\label{lem:wlansvc} $$WLANSvc $[C:\Windows\system32\svchost.exe -k] $$$ LocalSystemNetworkRestricted]

C:\Windows\System32\alg.exe Terminates process: Terminates process: C:\Windows\System32\VSSVC.exe
C:\Windows\System32\svchost.exe  ${\tt C:\Windows\Temp\ToggleService32.exe}$ 

Terminates process: Creates remote thread

#### Named Object Events

\Sessions\1\BaseNamedObjects\DBWinMutex
\BaseNamedObjects\MSDTC\_STATS\_EVENT
\BaseNamedObjects\{25FE086B-0970-4978-BF58-127731A00BE0}\_S-1-5-19 Creates mutex Creates mutex Creates mutex \BaseNamedObjects\WIATRACE MUTEX Creates mutex \BaseNamedObjects\ConsoleEvent-0x0000097C
\BaseNamedObjects\SvcctrlStartEvent\_A3752DX Creates event: Creates event \KernelObjects\MaximumCommitCondition \Security\LSA\_AUTHENTICATION\_INITIALIZED Creates event Creates event: Creates event: \BaseNamedObjects\TermSrvReadvEvent \BaseNamedObjects\RouterPreInitEvent \KernelObjects\SystemErrorPortReady Creates event Creates event: \...\WerSvcSystemPermissionsEvent \BaseNamedObjects\WiaServiceStarted Creates event:

#### File System Events

Creates: C:\Windows\Svstem32\output.txt

C:\Windows\System32\Msdtc\Trace\dtctrace.log
C:\Windows\ServiceProfiles\LocalService Creates: Creates

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

C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking Creates

Creates C:\ProgramData

```
C:\ProgramData\Microsoft\Crypto
C:\ProgramData\Microsoft\Crypto\RSA
  Creates:
 Creates:
                               C:\ProgramData\Microsoft\Crypto\RSA\
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
 Creates:
  Creates
 Creates:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f5eb1f2a398fce8997195383e42094df_577c175f-2428-49fc-a95e-635c93546ef9
 Creates:
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new} \\
 Creates:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
                               C:\Windows\Debug\WIA
 Creates:
 Onens:
                               C:\Windows\Prefetch\TOGGLESERVICE32_EXE-2248A864_nd
                               C:\Windows\System32
  Opens:
 Opens:
                               C:\Windows\Svstem32\sechost.dll
                               C:\Windows\System32\output.txt
C:\Windows\Prefetch\ALG.EXE-1D11534C.pf
  Opens:
 Opens:
                               C:\Windows\System32\at1.dll
C:\Windows\System32\wsock32.dll
 Opens:
  Opens:
 Opens:
                               C:\Windows\Svstem32\mswsock.dll
                               C:\Windows\System32\imm32.dll
C:\Windows\System32\en-US\alg.exe.mui
 Opens:
 Opens:
Opens:
                               C:\Windows\System32\rpcss.dl1
C:\Windows\System32\cryptbase.dl1
                               C:\Windows\System32\cryptsp.dll
C:\Windows\System32\rsaenh.dll
C:\Windows\Globalization\SortIng\SortDefault.nls
 Opens:
 Opens:
 Opens:
Opens:
                               C:\Windows\System32\RpcRtRemote.dll
C:\Windows\Prefetch\MSDTC.EXE-CC1DEC77.pf
 Opens:
                               C:\Windows\Svstem32\msdtctm.dll
                               C:\Windows\System32\msdtcprx.dll
C:\Windows\System32\mtxclu.dll
 Opens:
                               C:\Windows\System32\clusapi.dll
C:\Windows\System32\cryptdll.dll
  Opens:
  Opens:
 Opens:
                               C:\Windows\Svstem32\resutils.dll
                               C:\Windows\System32\version.dll
C:\Windows\System32\bcrypt.dll
  Opens:
 Opens:
  Opens:
                               C:\Windows\System32\ktmw32.dll
C:\Windows\System32\msdtclog.dll
  Opens:
 Opens:
                               C:\Windows\System32\winmm.dll
                               C:\Windows\System32\xolehlp.dll
C:\Windows\System32\dnsapi.dll
  Opens:
 Opens:
  Opens:
                               C:\Windows\System32\en-US\msdtc.exe.mui
C:\Windows\System32\comres.dll
  Opens:
 Opens:
                               C:\Windows\System32\msdtcVSp1res.dll
                               C:\Windows\System32\mtxoci.dll
  Opens:
                               C:\Windows\Svstem32\oci.dll
 Opens:
  Opens:
                               C:\Windows\system32\oci.dll
C:\Windows\system\oci.dll
 Opens:
 Opens:
                               C:\Windows\oci.dll
                               C:\Windows\System32\Wbem\oci.dll
  Opens:
                               C:\Windows\Svstem32\WindowsPowerShell\v1.0\oci.dll
 Opens:
  Opens:
                               C:\Windows\System32\Msdtc\Trace
C:\Windows\system32\MSDtc\trace\dtctrace.log
 Opens:
                               C:\Windows\System32\secur32.dll
C:\Windows\System32\sspicli.dll
 Opens
  Opens:
 Opens:
                               C:\Windows\Svstem32\credssp.dll
  Opens:
                               C:\Windows\DtcInstall.log
C:\Windows\System32\ntmarta.dll
 Opens:
                               C:\Windows\System32\Msdtc
C:\Windows\System32\Msdtc\MSDTC.LOG
 Opens
  Opens:
 Opens:
                               C:\Windows\Svstem32\en-US\msdtcVSp1res.dll.mui
  Opens:
                               C:\Windows\System32\FirewallAPI.dll
C:\Windows\Prefetch\UIODETECT.EXE-A794C8BB.pf
 Opens:
                               C:\Windows\System32\wtsapi32.dl1
C:\Windows\System32\winsta.dl1
 Opens
  Opens
 Opens:
                               C:\Windows\Svstem32\en-US\ui0detect.exe.mui
  Opens:
                               C:\Windows\System32\WlSOWndH.dll
C:\Windows\System32\ole32.dll
 Opens:
                               C:\Windows\system32\UIODetect.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-
  Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comct132.dll
                               C:\Windows\WindowsShell.Manifest
C:\Windows\System32\duser.dll
 Opens:
  Opens
 Opens:
                               C:\Windows\Svstem32\uxtheme.dll
                               C:\Windows\System32\dwmapi.dll
C:\Windows\System32\xmllite.dll
 Opens:
                               C:\Windows\System32\en-US\duser.dll.mui
C:\Windows\winsxs\x86_microsoft.windows.c
  Opens:
 Opens
controls resources 6595b64144ccf1df 6.0.7600.16385 en-us 581cd2bf5825dde9
Opens:
                               C:\Windows\System32\imageres.dll
C:\Windows\System32\en-US\imageres.dll.mui
  Opens:
 Opens:
                               C:\Windows\Fonts\StaticCache.dat
                               C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
  Opens:
 Opens:
  Opens:
                               C:\$Extend
                               C:\ProgramData
  Opens:
 Opens:
                               C:\ProgramData\Microsoft
                               C:\ProgramData\Microsoft\Crypto
C:\ProgramData\Microsoft\Crypto\RSA
  Opens:
 Opens:
  Opens:
                               C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
                               C:\Windows
  Opens:
                               C:\Windows\Globalization
 Opens:
  Opens:
                                 :\Windows\Globalization\Sorting
 Opens:
                               C:\Windows\Microsoft.NET
                               C:\Windows\ServiceProfiles
C:\Windows\ServiceProfiles\LocalService
  Opens:
  Opens:
 Opens
                               C:\Windows\ServiceProfiles\LocalService\AnnData
  Opens:
                               C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
 Opens:
                               C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c
 Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c\grouping
                               C:\Windows\System32\DriverStore
 Opens:
                               C:\Windows\System32\DriverStore\en-US
C:\Windows\System32\en-US
 Opens:
  Opens:
 Opens:
                               C:\Windows\System32\ntdll.dll
                               C:\Windows\System32\kernel32.dll
```

Creates

C:\ProgramData\Microsoft

```
Opens:
                                                                                         C:\Windows\Svstem32\apisetschema.dll
       Opens:
                                                                                         C:\Windows\System32\KernelBase.dll
                                                                                         C:\Windows\System32\locale.nls
       Opens:
                                                                                        C:\Windows\System32\svchost.exe
C:\Windows\System32\msvcrt.dll
      Opens:
       Opens:
      Opens:
                                                                                         C:\Windows\Svstem32\rpcrt4.dll
                                                                                        C:\Windows\System32\\DriverStore\en-US\ndiscap.inf_loc
C:\Windows\System32\userenv.dl1
       Opens:
      Opens:
                                                                                        C:\Windows\System32\profapi.dl1
C:\Windows\System32\gpapi.dl1
      Opens
       Opens:
      Opens:
                                                                                         C:\Windows\Svstem32\advapi32.dll
                                                                                        C:\Windows\System32\shell32.dl1
C:\Windows\System32\shlwapi.dl1
       Opens:
      Opens:
                                                                                        C:\Windows\System32\gdi32.dl1
C:\Windows\System32\user32.dl1
      Opens
       Opens:
      Opens:
                                                                                         C:\Windows\Svstem32\lpk.dll
                                                                                        C:\Windows\System32\usp10.dl1
C:\Windows\System32\msctf.dl1
       Opens:
      Opens:
                                                                                        C:\Windows\System32\en-US\svchost.exe.mui
C:\Windows\System32\pnrpsvc.dl1
      Opens:
       Opens:
                                                                                        C:\Windows\System32\crypt32.dll
C:\Windows\System32\msasn1.dll
C:\Windows\System32\en-US\crypt32.dll.mui
      Opens:
      Opens:
     Opens:
                                                                                        C:\WINDOWS\MICROSOFT.NET\NGENSERVICE_PRI1_LOCK.DAT
C:\Windows\System32\ncrypt.dll
                                                                                        C:\Windows\System32\p2pcollab.dl1
C:\Windows\System32\en-US\p2pcollab.dl1.mui
C:\Windows\System32\QAGENTRT.DLL
      Opens:
      Opens:
      Opens:
Opens:
                                                                                        C:\Windows\System32\DriverStore\en-US\netrast.inf_loc
C:\Windows\System32\en-US\dnsapi.dll.mui
      Opens:
                                                                                         C:\Windows\Svstem32\fveui.dll
                                                                                          C:\Windows\System32\en-US\fveui.dll.
       Opens:
\verb|C:\widetilde{W}| indows \\ Service \\ Profiles \\ Local Service \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ App Data \\ Roaming \\
      Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
                                                                                        C:\Windows\System32\ws2_32.dl1
C:\Windows\System32\nsi.dl1
       Opens:
      Opens:
       Opens:
                                                                                        C:\Windows\System32\wship6.dll
C:\Windows\System32\IPHLPAPI.DLL
      Opens:
      Opens:
                                                                                        C:\Windows\Svstem32\winnsi.dll
                                                                                          C:\Windows\System32\dhcpcsvc6.dll
       Opens:
                                                                                         C:\Windows\Svstem32\dhcpcsvc.dll
      Opens:
       Opens:
                                                                                        C:\Windows\System32\sqmapi.dll
C:\Windows\System32\ssdpapi.dll
       Opens:
      Opens:
  C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f6af2fef0fc5f4f2bc6f75c1ff7fd887_577c175f-2428-
49fc-a95e-635c93546ef9
      Opens:
                                                                                        C:\Windows\System32\p2psvc.dll
C:\Windows\System32\P2PGraph.dll
      Opens:
      Opens:
                                                                                         C:\Windows\Svstem32\esent.dll
                                                                                          C:\Windows\System32\slc.dll
       Opens:
      Opens:
                                                                                         C:\Windows\Svstem32\psapi.dll
       Opens:
                                                                                        C:\Windows\System32\oleaut32.dl1
C:\Windows\System32\DriverStore\en-US\nettcpip.inf_loc
      Opens:
      Opens
                                                                                         C:\Windows\Svstem32\authz.dll
       Opens
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\6bd89088524e6a41cf86084fbbab0cc6_577c175f-2428-
49fc-a95e-635c93546ef9
     Opens:
                                                                                         C:\Windows\System32\DriverStore\en-US\lltdio.inf_loc
      Onens
         .
VPROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\F0D041F93C731ACAA036AC2BD71BC124_577C175F-2428-
49FC-A95E-635C93546EF9
                                                                                         C:\Windows\System32\DriverStore\en-US\netsstpt.inf_loc
      Opens:
                                                                                         C:\Windows\System32\pnrpnsp.dll
      Opens:
      Opens
                                                                                         C:\Windows\System32\rasadhlp.dll
       Opens
. . \dot{r} \\ C: 
     Opens:
C: \windows \ensuremath{\backslash} Service \ensuremath{\backslash} Poer \ensuremath{\backslash} Networking \ensuremath{\backslash} 8d844364c535c5b5c8ba03cedd538a73.sst.new \ensuremath{\backslash} Networking \ensurema
       Opens:
C:\windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\8d844364c535c5b5c8ba03cedd538a73.sst
                                                                                        C:\Windows\System32\Wldap32.dll
C:\Windows\System32\schannel.dll
      Opens:
      Opens:
                                                                                         C:\Windows\System32\DriverStore\en-US\netserv.inf_loc
C:\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\ROAMING\PEERNETWORKING\65E9EDA7BCB6088518AEA0DDF13DF80843A6EA25.HOMEGROUPCLASSIFIER\F8D4F95592CE335421D51FAD88712F5C\GROUPING\TMP.EDB
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c\grouping\db.mdb
                                                                                        C:\Windows\Temp
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp
      Opens:
       Opens:
      Opens:
 C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f5eb1f2a398fce8997195383e42094df_577c175f-2428-
49fc-a95e-635c93546ef9
     Opens:
                                                                                         C:\Windows\System32\en-US\QAgentRT.dll.mui
       Opens
C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
C:\Windows\System32\powrprof.dll
      Opens:
      Opens:
                                                                                        C:\Windows\System32\en-US\spoolsv.exe.mui
C:\Windows\System32\en-US\setupapi.dll.mui
       Opens:
      Opens:
      Opens:
                                                                                         C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
                                                                                        C:\Program Files
C:\Program Files\DVD Maker
       Opens:
      Opens:
                                                                                        C:\Program Files\DVD Maker\Shared
C:\Program Files\DVD Maker\Shared\DvdStyles
       Opens:
       Opens:
      Opens:
                                                                                         C:\Users
       Opens:
                                                                                          C:\Users\Admin
      Opens:
                                                                                         C:\Users\Admin\AppData
                                                                                        C:\Users\Admin\AppData\Local
C:\Users\Admin\AppData\Local\Microsoft
       Opens:
       Opens:
                                                                                         C: \space{-0.05\line Normal Normal
      Opens
       Opens:
                                                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
      Opens:
Files\Content.IE5
                                                                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
      Opens:
Files\Content TE5\KO5TVCON
     Opens:
                                                                                        C:\Windows\System32\drivers\etc\lmhosts
                                                                                        C: Wisers\Admin\AppData\Roaming
C: Ulsers\Admin\AppData\Roaming
Microsoft
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\Wy
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My
C:\Users\Admin\AppData\Roaming\Microsoft\Windows
     Opens:
       Opens:
      Opens:
      Opens:
       Opens:
      Opens:
                                                                                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
                                                                                         C:\Windows\Fonts
```

```
Opens:
                               C:\Windows\IME
  Opens:
                               C:\Windows\IME\IMEJP10
                               C:\Windows\Microsoft.NET\Framework
  Opens:
 Opens:
                               C:\Windows\Microsoft.NET\Framework\v2.0.50727
  Opens
                               C:\Windows\SoftwareDistribution
 Opens:
                               C:\Windows\SoftwareDistribution\WuRedir
Opens:
9A65BC822C77
                               C:\Windows\SoftwareDistribution\WuRedir\9482F4B4-E343-43B6-B170-
 Onens
                               C:\Windows\System32\catroot
                               C:\Windows\System32\catroot2
  Opens:
 Opens:
                               C:\Windows\Svstem32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
                               C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
C:\Windows\System32\com
  Opens:
 Opens:
                               C:\Windows\System32\SMI
C:\Windows\System32\SMI\Store
 Opens:
  Opens:
 Opens:
                               C:\Windows\Svstem32\rasctrs.dll
                               C:\Windows\System32\VSSVC.exe
C:\Windows\System32\vssapi.dll
  Opens:
 Opens:
                               C:\Windows\System32\vsstrace.dll
C:\Windows\System32\netapi32.dll
 Opens:
  Opens:
 Opens:
                               C:\Windows\Svstem32\netutils.dll
                               C:\Windows\System32\srvcli.dll
C:\Windows\System32\wkscli.dll
 Opens:
 Opens:
                               C:\Windows\System32\samcli.dll
C:\Windows\System32\setupapi.dll
                               C:\Windows\System32\cfgmgr32.dll
C:\Windows\System32\devobj.dll
C:\Windows\System32\virtdisk.dll
 Opens:
 Opens:
 Opens:
Opens:
                               C:\Windows\System32\fltLib.dll
C:\Windows\System32\en-US\VSSVC.exe.mui
 Opens:
                               C:\Windows\Svstem32\clbcatq.dll
                               C:\Windows\System32\vss_ps.dll
C:\Windows\System32\en-US\vsstrace.dll.mui
 Opens:
 Opens:
Opens:
                               C:\Windows\System32\samlib.dl1
C:\Windows\System32\es.dl1
 Opens:
                               C:\Windows\System32\propsys.dll
                               C:\Windows\System32\catsrvut.dll
C:\Windows\System32\mfcsubs.dll
  Opens:
 Opens:
  Opens:
                               C:\Windows\System32\sxs.dll
C:\Windows\System32\eventcls.dll
  Opens:
 Opens:
                               C:\Windows\System32\stdole2.tlb
                               C:\Windows\System32\msxm13.dll
C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:
 Opens:
  Opens:
                               C:\Windows\System32\msxm13r.dl1
C:\Windows\System32\wintrust.dl1
  Opens:
 Opens:
                               C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
00C04FC295EE}\catdb
                               C:\Windows\Svstem32\catroot2\{F750E6C3-38EE-11D1-85E5-
 Opens
00C04FC295EE}\catdb
                               C:\Windows\System32\catroot2\edb.chk
 Opens:
 Opens:
                               C:\Windows\System32\sdclt.exe
C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\ADMIN@DEMDEX[2].TXT
Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\CONTENT.IE5\KQSTVCON\LOCALE-SPECIFIC[1].CSS
                               C:\Windows\Fonts\palab.ttf
C:\WINDOWS\SYSTEM32\CATROOT\TMP1E1E.TMP
 Onens
  Opens:
 Opens:
                               C:\WINDOWS\SYSTEM32\CATROOT\TMP1E09.TMP
Opens: C:\\
9A65BC822C77\WUREDIR.CAB.BAK
                               C:\WINDOWS\SOFTWAREDISTRIBUTION\WUREDIR\9482F4B4-E343-43B6-B170-
 Onens:
                               C:\WINDOWS\SYSTEM32\CATROOT\TMP26E3 TMF
                               C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
  Opens:
 Opens:
                               C:\Windows\Svstem32\wersvc.dll
  Opens:
                               C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
C:\CONFIG.MSI
 Opens:
                               C:\CONETG MST\41EA3 RBE
 Opens:
                               C:\CONFIG.MSI\41F56.RBF
  Opens:
 Opens:
                               C:\Windows\System32\wiaservc.dll
  Opens:
                               C:\Windows\System32\msv1_0.dl1
C:\CONFIG.MSI\41F57.RBF
 Opens:
 Opens:
                               C:\Windows\System32\wiatrace.dll
C:\Windows\debug\WIA\wiatrace.log
 Opens:
                               C:\Windows\Svstem32\drivers\nwifi.svs
  Opens:
                               C:\Windows\AppPatch\drvmain.sdb
C:\Windows\System32\drivers\ndisuio.sys
  Opens:
                               C:\Windows\System32\output.txt
C:\Windows\System32\Msdtc\Trace\dtctrace.log
 Writes to
  Writes to:
 Writes to:
                               C:\Windows\System32\Msdtc\MSDTC.LOG
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f5eb1f2a398fce8997195383e42094df_577c175f-2428-
49fc-a95e-635c93546ef9
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
 Writes to:
                               C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608
00C04FC295EE}\catdb
 Writes to:
                               C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\catdb
                               C:\Windows\Svstem32\output.txt
 Reads from:
                               C:\Windows\Fonts\StaticCache.dat
C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
  Reads from
  Reads from
  Reads from
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sstart} \\
 Reads from:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Readsfrom: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
                               C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
Network Events
```

DNS query:	WPAD	
Connects to:	10.74.7.255:138	
Connects to:	10.74.7.255:137	
Sends data to:	10.74.7.255:138	
Sends data to:	10.74.7.255:137	
Receives data from:	10.74.7.100:138	
Receives data from:	10.74.7.100:137	

## Windows Registry Events

Creates key:  $\label{thm:linear} \begin{tabular}{ll} HKLM\software\mbox{\sc microsoft\windows} & nt\current\version\peernet\pnrp\ipv6-relation\peernet\pnrp\poer$ 

linklocal\linklocal\_ff00::%11/8

HKCU\software\classes\local settings\muicache\27\52c64b7e Creates key:

HKCU\software\classes\local settings\muicache
HKLM\system\currentcontrolset\control\deviceclasses\\\ 65a9a6cf-64cd-480b-Creates key

```
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
32c86e1ba19f}\control
                                                 HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
   Creates key:
843e - 32c86e 1ba19f\} \\ \text{\#?\#umb\#umb\#1\&841921d\&0\&printerbusenumerator\#\{65a9a6cf-64cd-480b-843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e-1844e
32c86e1ba19f}\#\control
  Creates kev:
                                                 HKLM\system\currentcontrolset\control\deviceclasses
   Creates key
                                                 HKLM\system\currentcontrolset\services\umbus\end
                                                 HKLM\software\classes
   Creates key:
   Creates key
                                                 HKLM\svstem\currentcontrolset\services\vss\diag\registry writer
                                                  HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
   Creates key
   Creates key
                                                 HKLM\system\currentcontrolset\services\vss\diag\asr writer
   Creates key:
                                                 HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization
writer
  Creates key
                                                 HKLM\svstem\currentcontrolset\control\stillimage\trace
   Creates key
                                                  HKLM\system
   Creates key
                                                 HKLM\svstem\currentcontrolset
                                                 HKLM\system\currentcontrolset\control
HKLM\system\currentcontrolset\control\stillimage
   Creates key
   Creates key:
   Creates key
                                                 Creates key:
  Creates key
                                                 HKLM\system\currentcontrolset\enum\root\legacy_nativewifip
                                                 HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000\control
   Creates key:
   Creates key:
   Creates key:
                                                 HKLM\system\currentcontrolset\services\nativewifip\parameters
HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters
   Creates key
   Creates key
                                                 HKLM\svstem\currentcontrolset\services\nativewifip
Creates key:
08002be10318}\0005
                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Creates key:
08002be10318}\0008
                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Creates key
08002be10318}\0006
                                                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Creates key:
08002be10318}\0007
   Creates key:
                                                  HKLM\system\currentcontrolset\services\ndisuio\enum
   Creates key
                                                 HKLM\system\currentcontrolset\enum\root\legacy_ndisuio
                                                  HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000
   Creates key
   Creates key:
   Creates key:
   Creates key:
08002be10318}\0000
Creates key:
08002be10318}\0003
Creates key:
08002be10318}\0004
                                                 Creates key
08002be10318}\0002
   Creates key:
08002be10318}\0001
```

HKLM\system\currentcontrolset\enum\root\legacy\_ndisuio\0000\control HKLM\system\currentcontrolset\services\ndisuio
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

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

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

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

Creates key: 08002be10318}\0011 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

Creates key: 08002be10318}\0009 HKLM\system\currentcontrolset\services\umbus\enum[1]

Deletes value: Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKIM\system\currentcontrolset\control\terminal server HKLM\system\currentcontrolset\control\safeboot\option Opens key: Opens kev: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens key: HKCII/

Opens key:  ${\tt HKCU \backslash control\ panel \backslash desktop \backslash muicached \backslash machine language configuration}$ Opens key: HKLM\software\policies\microsoft\mui\settings

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

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

Opens key: HKLM\software\microsoft\windows\currentversion\sidebvside Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

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

HKLM\Software\milcrusoft\varioussit\currenteession\dagasstacs
HKLM\Software\milcrusoft\vrpc
HKLM\system\currentcontrolset\control\computername\activecomputername Opens key:

Opens key:

Opens key: HKLM\system\setup
HKLM\software\policies\microsoft\windows nt\rpc

Opens key:

HKLM\software\policies\microsoft\sqmclient\windows
HKLM\software\microsoft\sqmclient\windows Opens key: Opens key: Opens kev: HKLM\svstem\currentcontrolset\control\samservicelist

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
HKLM\system\currentcontrolset\control\error message instrument Opens key: Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\system\currentcontrolset\control\mui\settings HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
HKLM\software\microsoft\ole

Opens key: Opens key: Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\microsoft\oleaut HKCU\software\classes\ Opens key: Opens key: Opens key: HKLM\software\classes
HKLM\software\microsoft\com3

Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da} Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\treatas HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\progid Opens key: Opens key: Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprocserver32 HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler32 Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler

Opens key: HKCR\appid\alg.exe

HKLM\software\microsoft\ole\appcompat Opens key: Opens key:

HKLM\system\currentcontrolset\control\lsa
HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong Opens key

cryptographic provider Opens key:

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

HKLM\software\policies\microsoft\cryptography Opens key: Opens key: HKLM\software\microsoft\cryptography
HKLM\software\microsoft\cryptography\offload

Opens key: Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}

Opens key: Opens key:

Opens key: HKLM\svstem\currentcontrolset\services\bfe

Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key:  $\label{thm:local-hammon} HKLM \software \microsoft \sqmclient \windows \disabled sessions \hkCR\clsid \f8ade1d3-49df-4b75-9005-ef9508e6a337\}$ 

```
HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
   Opens key
                                                    HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
    Opens key:
    Opens key:
    Opens key:
                                                     HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
    Opens key:
                                                    HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
   Opens key:
                                                    HKCR\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
HKLM\software\microsoft\alg\isv
    Opens key:
    Opens key:
   Opens key
                                                     HKLM\software\microsoft\msdtc\tracing
    Opens key:
                                                     HKLM\software\microsoft\msdtc\tracing\sources
                                                     HKLM\software\microsoft\msdtc\tracing\output
   Opens key:
    Opens key:
                                                     HKLM\software\microsoft\msdtc
                                                     HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc
    Opens key:
    Opens key
                                                     HKCR\cid local
    Opens key:
                                                     HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a
   Opens key:
                                                     HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\description
                                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\description
    Opens key:
    Opens key:
    Opens key:
                                                     HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5
    Opens key:
                                                     HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5\description
   Opens key:
                                                     HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9
                                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\description
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed
    Opens key:
    Opens key:
   Opens key:
                                                     HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\description
                                                     HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid
   Opens key:
                                                    HKCR\svcid.local
                                                    HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\host
    Opens key:
    Opens key:
   Opens key:
                                                    \label{eq:hkcr_cid.local_dr77da18-5d11-4ac9-b6c0-782ab52d45ed\\ \label{eq:hkcr_svcid.local_dr88091f0-bff6-11ce-9de8-00aa00a3f464} \\ \text{defaultprovider}
   Opens key:
                                                     HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\protocol
                                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\endpoint

HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\customproperties
    Opens key:
    Opens key:
    Opens key:
Opens key:
                                                     HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\customproperties\log
                                                     HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
782ab52d45ed\customproperties\log\size
                                                    HKLM\software\microsoft\msdtc\mtxoci
HKLM\software\microsoft\msdtc\security
    Opens key:
    Opens key:
                                                    \label{thm:hklmsoftware} HKLM \software \microsoft \windows nt \current version \asr \restores ession \ HKCR \cid.local \d777da18-5d11-4ac9-b6c0-
    Opens key
    Opens key:
782ab52d45ed\customproperties\log\path
Opens key: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions
   Opens key:
Opens key:
                                                    HKLM\system\currentcontrolset\control\minint
HKLM\system\currentcontrolset\control\timezoneinformation
   Opens key:
                                                    HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules
                                                     HKLM\software\microsoft\windows
    Opens key:
nt\currentversion\tracing\msdtc\modules\transaction transitions
   Opens key:
Opens key:
                                                    HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed HKLM\software\microsoft\windows nt\currentversion
   Opens kev
                                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\svcid
                                                    HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\host
    Opens key:
   Opens key:
   Opens key:
Opens key:
                                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\clsid
HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
   Opens key
                                                     HKCR\cid local\b90b59d3-8bb9-4d71-af93-3faf363251c9\protocol
                                                     HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\endpoint
    Opens key:
   Opens key:
                                                     HKCU\control panel\international
    Opens key:
                                                    HKLM\system\currentcontrolset\control\nls\customlocale HKLM\system\currentcontrolset\control\nls\extendedlocale
    Opens key:
    Opens key
                                                    \label{thm:local} HKLM \copt which is a control set of the microsoft through the microsoft of the microsof
    Opens key:
   Opens key:
                                                    HKLM\svstem\currentcontrolset\control\securityproviders
    Opens key:
                                                    HKLM\system\currentcontrolset\control\lsa\sspicache
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
   Opens key:
    Opens key:
                                                    HKLM\system\currentcontrolset\control\securityproviders\saslprofiles HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\customproperties
    Opens key:
   Opens key:
                                                     HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\customproperties\dac
    Opens key:
                                                    HKLM\system\currentcontrolset\control\lsa\accessproviders
HKLM\system\currentcontrolset\services\ldap
   Opens key:
    Opens key:
                                                     HKCR\cid local\199661d8-979c-4ebb-9e3e-a23014be3f1a\svcid
                                                     HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef
    Opens key:
                                                    HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\host

HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\clsid

HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider
   Opens key:
    Opens key
   Opens key:
                                                    \label{local199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol\\ HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\endpoint\\ \end{center}
    Opens key:
    Opens key:
   Opens key:
                                                     HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\svcid
    Opens key
                                                    HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\host
   Opens key:
                                                    \label{thm:hkcr_cid.local} $$HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\\ HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\\ defaultprovider $$HKCR\svcid.local\81a3a129-619d-4d5f-a782-28d960ea489d\\ HKCR\svcid.local\81a3a129-619d-4d5f-a782-28d960ea489d\\ HKCR\svcid.local\81
    Opens key:
    Opens key:
   Opens key:
                                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\protocol
    Opens key:
                                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\endpoint
HKLM\software\microsoft\windows\windows error reporting\wmr
    Opens key:
   Opens key:
Opens key:
                                                    HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4\}
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4\}\treatas
   Opens key:
                                                     HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
    Opens key:
                                                    HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
    Opens key:
    Opens key:
                                                    HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
HKLM\system\currentcontrolset\control\computername
    Opens key:
   Opens kev
                                                    HKU\.default\control
 panel\desktop\muicached
                                                   machinelanguageconfiguration
                                                    HKU\.default\software\policies\microsoft\control panel\desktop
   Opens kev:
                                                    HKUV.default\control panel\desktop\languageconfiguration
    Opens key:
    Opens key:
                                                    HKU\.default\control panel\desktop\muicached
HKU\.default\control panel\international
HKLM\software\microsoft\ctf\compatibility\ui0detect.exe
    Opens key
    Opens key:
    Opens key:
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x0000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
   Opens key
                                                    HKI M\software\microsoft\ctf\
    Opens key:
                                                     HKLM\software\microsoft\ctf\knownclasses
   Opens key
HKLM\software\microsoft\directui
   Opens key:
    Opens key:
                                                    HKLM\svstem\currentcontrolset\control\nls\locale
    Opens key:
                                                     HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens kev:
                                                    HKLM\system\currentcontrolset\control\nls\language groups
    Opens key:
                                                    HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
                                                    HKLM\software\microsoft\windows
    Opens key:
nt\currentversion\languagepack\datastore_v1.0
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
                                                    HKLM\software\microsoft\windows
```

```
nt\currentversion\languagepack\surrogatefallback\segoe ui
                            HKLM\software\microsoft\windows nt\currentversion\svchost
HKLM\software\microsoft\windows
  Opens key
 Opens key:
nt\currentversion\svchost\localservicepeernet
Opens key: HKLM\system\currentcontrolset\services
 Opens key:
 Opens key:
                            HKLM\svstem\currentcontrolset\services\p2pimsvc
  Opens key:
                            HKLM\system\currentcontrolset\services\p2pimsvc\parameters
HKLM\software\microsoft\windows nt\currentversion\winlogon
 Opens key:
 Opens key:
                            HKLM\software\policies\microsoft\windows\system
  Opens key:
                             HKLM\software\policies\microsoft\peernet
 Opens key:
                            HKLM\svstem\currentcontrolset\services\pnrpsvc
  Opens key:
                            HKLM\system\currentcontrolset\services\pnrpsvc\parameters
                            HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
 Opens key:
                            HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog\2c69d9f1-3a1fc5ac
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000000
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000004
 Opens key:
\label{local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-loc
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000000
Opens kev:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000012
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000016
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000017
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key: 
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
 Opens key:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000001
Opens kev:
Opens key:
Opens key:
                            HKLM\system\currentcontrolset\services\winsock\parameters
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:
  Opens key:
                            HKLM\system\currentcontrolset\services\winsock\setup migration\providers
                            HKLM\system\currentcontrolset\services\winsock\setup
 Opens kev
migration\providers\tcpip6
  Opens key:
                            {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ parameters \verb|\ interfaces | \\
 Opens key:
c19ce8a73253}
Opens key: '
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
 Opens key:
                            HKLM\svstem\currentcontrolset\services\tcpip\linkage
  Opens key:
                            HKLM\software\microsoft\sqmclient
                            HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp
 Opens key:
  Opens key:
                            HKLM\software\policies\microsoft\peernet\pnrp\ipv6-linklocal
                            HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
 Opens key:
linklocal
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
a03a-e3ef65729f3d3
 Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
```

```
Opens kev:
                                                                         HKCU\software\microsoft\windows\currentversion\explorer
     Opens key:
                                                                         \label{thm:cu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \session in folding the context of the con
     Opens key:
     Opens key
                                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
  folders
    Opens key:
                                                                         HKLM\software\microsoft\windows nt\currentversion\profilelist
                                                                        HKLM\system\currentcontrolset\control\session manager\environment HKLM\software\microsoft\windows\currentversion
     Opens key:
     Opens key:
     Opens key
                                                                         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
     Opens key:
                                                                         HKCU\environment
     Opens key:
                                                                         HKCU\volatile environment
                                                                        HKCU\volatile environment\0
HKLM\software\policies\microsoft\windows\explorer
     Opens key:
     Opens key:
     Opens key:
                                                                         HKCU\software\policies\microsoft\windows\explorer
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
 9afe-ea3317b67173}
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
    Opens kev:
                                                                        HKLM\system\currentcontrolset\services\crypt32
                                                                        HKLM\software\microsoft\cryptography\oid\
HKLM\software\microsoft\cryptography\oid\encodingtype 0
     Opens key:
Opens key:
0\certdllopenstoreprov
                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
    Opens kev:
                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
Opens key:

Ocertdllopenstoreprovldap

Onens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
 1\certdllopenstoreprov
                                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
     Opens key
0\cryptdlldecodeobjectex
                                                                         {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype \\
1\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
                                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
     Onens key
                                                                        HKLM\software\microsoft\crvptographv\oid\encodingtvpe
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
                                                                         {\tt HKLM \ } software \verb|\ microsoft \ \\ cryptography \verb|\ oid \ \\ encoding type \\ encoding typ
1\crvptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
     Opens kev:
                                                                        HKLM\software\microsoft\windows nt\currentversion\msasn1
                                                                        HKLM\software\microsoft\cryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\provider\microsoft\ryptography\defaults\
     Opens key:
     Opens key
schannel cryptographic provider
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}
     Opens kev:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82 - fdc1 - 4dc3 - fdc1 - fd
a9dd-070d1d495d97}\propertybag
                                                                        \label{thm:hammon} HKLM\software\microsoft\cryptography\deshashsessionkeybackward\ HKLM\software\microsoft\cryptography\oid\encodingtype
     Opens key:
     Opens key
0\cryptdllfindoidinfo
Opens key: HKLM\software\microsof
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7
                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
               ns key:
                                                                         HKLM\system\currentcontrolset\control\mui\stringcachesettings
     Opens key:
                                                                         HKCU\software\classes\local settings\muicache\27\52c64b7e
     Opens kev:
                                                                         HKCU\software\classes\local settings\muicache
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7
    Opens key:
Opens key:
                                                                         HKLM\svstem\currentcontrolset\control\deviceclasses
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#\65a9a6cf-64cd-480b-843e-
32c86e1ba19f}
     Opens key:
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
 32c86e1ba19f}\#
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
    Opens key:
b082-00a0c91efb8b}
Opens key:
b082-00a0c91efb8b}\##?
                                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
 #pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&6373acf&0&400008#{2accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accfe60-b0accf
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&080#{2accfe60-c130-11d2-b082-00a0c91efb8b}
                                                                        HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
    Opens kev:
HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
     Opens kev:
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2d9c6e01&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&1#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key:
84ae-d30803bae505}
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
    Opens key
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
84ae-d30803bae505}\##?#
                                                                      oot#vdrvroot#0000#{2e34d650-5819-42ca-84ae-d30803bae505}
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
    Opens key:
bc8c-00a0c91405dd}
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
     Opens key:
bc8c-00a0c91405dd}\##?#acpi#pnp0f03#481d401fb580#1378de44c-56ef-11dl-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11dl-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co102#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-
00a0c91405dd}
                                                                         HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
    Opens key:
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co102#6&1e20eb37&0&0001#{378de44c-56ef-11d1-bc8c
00a0c91405dd}
     Opens key:
                                                                        HKLM\svstem\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col03#6&1c83c2e&0&0002#{378de44c-56ef-11d1-bc8c
```

00a0c91405dd} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\#;?#hid#vid\_14dd&pid\_1005&col03#6&1e20eb37&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd} Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{3bc8c-00a0c91405dd}\##?#root#rdp\_mou#0000#{378de44c-56ef-11d1-bc8c-00a0c91405dd} Opens key: 8a92-1e6861e6af27} HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Opens key HKI M\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27c8&subsys\_01e61028&rev\_01#3&2411e6fe&0&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\\##?#pci#ven\_8086&dev\_27c8&subsys\_01e61028&rev\_01#3&2411e6fe&1&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-4\)
8a92-1e6861e6af27}\\##?#pci#ven\_8086&dev\_27c9&subsys\_01e61028&rev\_01#3&2411e6fe&0&e9#{3abf6f2d-HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-71c4-462a-8a92-1e6861e6af27} HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Opens key: 8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27c9&subsys\_01e61028&rev\_01#3&2411e6fe&1&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens kev: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27ca&subsys\_01e61028&rev\_01#3&2411e6fe&0&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-46 8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27ca&subsys\_01e61028&rev\_01#3&2411e6fe&1&ea#{3abf6f2d-HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\\##?#pci#ven\_8086&dev\_27cc&subsys\_01e61028&rev\_01#3&2411e6fe&0&ef#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-46 8a92-1e6861e6af27}\##?#pci#yen\_8086&dev\_27cc&subsys\_01e61028&rev\_01#3&2411e6fe&1&ef#{3abf6f2d-HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-71c4-462a-8a92-1e6861e6af27} HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662-Opens key: b732-99a6111edc0b} Opens key: a5d6-28db04c10000} HKLM\svstem\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{ a5d6-28db04c10000} \##?#root#system#0000#{4747b320-62ce-11cf-a5d6-28db04c10000} Opens key: be5e-00a0c9062857} HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-Opens kev: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e-00a0c9062857} HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-Opens key:  $Opens\,key: \qquad \qquad \text{HKLMN-system} \\ \text{tontrol-set} \\ \text{control-device} \\ \text{color-good-second} \\ \text{tond-secon$ Opens key: 88cb-001111000030} HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid\_14dd&pid\_1005&col01#6&1c83c2e&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-1' 88cb-001111000030}\\##?#hid#vid\_14dd&pid\_1005&col01#6&1e20eb37&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030} 001111000030} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-88cb-001111000030}\##?#hid#vid\_14dd&pid\_1005&col02#6&1c83c2e&0&0001#{4d1e55b2-f16f-11cf-88cb 001111000030} Opens key: HKLM\system\currentcontrolset\control\devicecidsses\tquiessus\tqu

HKLM\svstem\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-

001111000030} Onens key HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-

88cb-001111000030}\##?#hid#vid\_14dd&pid\_1005&co103#6&1c83c2e&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-00111100030}\#;?#hid#vid\_14dd&pid\_1005&col03#6&1e20eb37&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}

Opens key: 94f2-00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-Opens key: 94f2-00a0c91efb8b}\##?  $HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f56307-b6bf-11d0-b6b$ 

#ide#diskhitachi 3.5.1.9 #5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b} Opens key: 94f2-00a0c91efb8b}\##? HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-

#ide#diskvbox\_harddisk \_\_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d 94f2-00a0c91efb8b}\##?#scsi#disk&ven\_dell&prod\_virtual\_disk#6&17b13437&0&000000#{53f56307-b6bf- $HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f56307-b6bf-11d0-b6b$ 

11d0-94f2-00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-Opens key:

11d0-94f2-00a0c91efb8b} Opens kev: HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-

94f2-00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-Opens key:

Opens key: https://de/carbmil-dt-st\_dvd-rom\_gdrt100\_\_\_\_\_\_\_1.02\_\_\_\_#5&28836b88&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: httln://dvd-rom\_gdrt100\_\_\_\_\_\_\_\_1.05\_\_\_\_#5&28836b88&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
##?#ide#cdromhl-dt-st\_dvd-rom\_gdrt100\_\_\_\_\_\_\_\_1.05\_\_\_\_#5&23a61b2180&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromvbox\_cd-#5&106af171&0&1.0.0#{53f56308-b6bf-11d0-94f2-1.0 rom

00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-Opens kev:

94f2-00a0c91efb8b}\##?#ide#cdromvbox\_cd-rom\_ 00a0c91efb8b}

Opens key: 94f2-00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-

9472-00a0c91erb88}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st\_dvd-rom\_gdrt10n\_\_\_\_\_\_1.02\_\_\_#5828836b880&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} 94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st\_dvd-rom\_gdr-

\_\_1.05\_\_\_#5823a61b2180&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0t10n\_ Opens key: 94f2-00a0c91efb8b}\##?#ide#cdromvbox\_cd-

\_\_1.0\_\_ \_#5&106af171&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\cur 94f2-00a0c91efb8b}\##?#ide#cdromvbox\_cd-HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-1 0 #5&394c0ad3&0&0.1.0#{53f5630d-b6bf-11d0-94f2-

HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-Opens kev:

rom 00a0c91efb8b}

94f2-00a0c91efb8b}\##?#storage#volume#{69d250e0-6c18-11e3-b3bc

```
806e6f6e6963\#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLMN\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{69d250e0-6c18-11e3-b3bc-
806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#0000000000007e00#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\device 94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-806e6f6e6963}#00000075343e000#{53f5630d-b6bf-11dd-94f2-00a0c91efb8b}
                                        HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f447-11df-aef6-
806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#;?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e963}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\
94f2-00a0c91efb8b\\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#000000211262e800#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\device 94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-806e6f6e6963}#0000002131c36880#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM/system/currentcontrolset/control/deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#;?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#00000000000000000000#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\
94f2-00a0c91efb8b\\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#00000075343e000#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key. mkLm/systemicurrentcontroliset/controlidevice 94f2-00a0c91efb8b}\##2#storage/wolume#{e29ac6c3-7037-11de-816d-806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?#storage#volume#{e29ac6c3-7037-11de-816d-806e6f6e6963}#0000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-
94f2-00a0c91efb8b\\##?#storage#volume#\\e29ac6c3-7037-11de-816d-
806e6f6e6963\\#00000020f3026800#\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\##?#storage#volume#\{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000000211262e800#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrol\set\control\\
94f2-00a0c91efb8b\\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Onens key
                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot10#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?\storage\volumesnapshot\harddiskvolumesnapshot11\#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d 94f2-00a0c91efb8b}\\##?#storage#volumesnapshot#harddiskvolumesnapshot2#{53f5630d-b6bf-11d0-94f2-
                                         00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f563ud-obob-ii
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f563ud-b6bf-11d0-94f2
                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11c94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2-
                                         00a0c91efb8b}
Opens kep: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\#?#storage#volumesnapshot#harddiskvolumesnapshot6#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d 94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-
                                          00a0c91efb8b}
                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Opens key:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot8#{53f5630d-b6bf-11d0-94f2
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key:
94f2-00a0c91efb8b}
                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
  Opens kev:
94f2-00a0c91efb8b}\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}
                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
  Opens key:
85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\con
                                         HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
f2f2-4f3b-85bb-30ff1f953599}
                                        HKLM\svstem\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
  Opens key:
85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&2e5a831d&0&28f0#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f85bb-30ff1f953599}\##?#pci#ven_80ee&dev_beef&subsys_0000000&rev_00#3&267a616a&0&10#{5b45201d-
                                        HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\\ (65a9a6cf-64cd-480b-843e-32c86e1ba19f\)\##?#root#umbus#0000#\\\(65a9a6cf-64cd-480b-843e-32c86e1ba19f\)\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
32c86e1ba19f}\#\control
Opens key:
bcf7-00aa00b7b32a}
                                          HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
Openskey: HKLM\system\currentcontrolset\control\deviceclasses bcf7-00aa00b7b32a}\##?#acpi#pnp0c0a#0#{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
                                          HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
  Opens kev:
                                          HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
a537-0000f8753ed1}
                                         HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
  Opens key:
a537-0000f8753ed1}\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-
0000f8753ed1}
  Opens kev:
                                          HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}
```

```
Opens key:
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
 b7df-24c5d8a8ccb8}\##?#display#default_monitor#4&2abfaa30&0&12345678&00&02#{866519b5-3f07-4c97
 b7df-24c5d8a8ccb8}
    Opens kev:
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
 b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2dcf5eab&0&12345678&06&05#{866519b5-3f07-4c97-
 b7df-24c5d8a8ccb8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\\##?#display#default_monitor#582fab8e3980&12345678&06805#{866519b5-3f07-4c97-
 h7df-24c5d8a8cch83
 Opens key:
bc8c-00a0c91405dd}
                                                     HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#acpi#pnp0303#4&1d401fb5&0#(884b96c3-56ef-11d1-bc8c-00a0c91405dd)\#P;#acpi#pnp0303#4&1d401fb5&0#(884b96c3-56ef-11d1-bc8c-00a0c91405dd)\#P;#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
 00a0c91405dd}
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\#;?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&000#{884b96c3-56ef-11d1-bc8c-
 00a0c91405dd}
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{8 bc8c-00a0c91405dd}\##?#root#rdp_kbd#0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
 Opens key:
af1f-0000f800845c}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-af1f-0000f800845c}\##?#acpi#pnp0400#4&1d401fb580#{97f76ef0-f883-11d0-af1f-0000f80845c}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
   Opens kev:
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
 359c-8bef029dbdd0}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
   Opens key:
 359c-8bef029dbdd0}\##?#acpi#genuineintel_-_x86_family_6_model_15_-
_intel(r)_xeon(r)_cpu____x3220_@_2.40ghz#_1#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
| Opens key: | HKLM\system\currentcontrolset\control\deviceclasses\\97fadb10-4e33-40ae-359c-8bef029dbdd0}\\##?#acpi#genuineintel_-x86_family_6_model_15_-
_intel(r)_xeon(r)_cpu____x3220__@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
intel(r)_xeon(r)_cpu x3220_@_2.4ugnz#_Z#{9/Tad010-4e33-4uae-359c-8oe7u2youuuuy}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\##?#acpi#genuineintel_-_x86_family_6_model_15_-
intel(r)_xeon(r)_cpu x3220_@_2.40ghz#_3#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34a9bc#{a5dcbf10-6530-11d2-901f-
 00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10}901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#fac72212e15ea84#{a5dcbf10-6530-11d2-901f-
                                                    00c04fb951ed}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
    Opens kev:
 8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0
8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{ad498944-
                                                    762f-11d0-8dcb-00c04fc3358c)
                                                   HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
    Opens kev:
 8dcb-00c04fc3358c\} \\ \text{\#?\#pci\#ven\_14e4\&dev\_1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad498444-1659\&subsys\_01e61028\&rev\_11\#\{ad498444-1659\&subsys\_01e61028\&rev\_11\#\{ad498444-1659\&subsys\_01e61028\&rev\_11\#\{ad4984444\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_11640444\&rev\_11640444\&rev\_11640444\&rev\_11640444\&rev\_11640444\&rev\_11640444\&rev\_1164044\&rev\_11640444\&rev\_11640444\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044\&rev\_1164044
 762f-11d0-8dcb-00c04fc3358c}
   Onens key:
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad498944
 762f-11d0-8dcb-00c04fc3358c}
 Opens~key: HKLM \system \current control \system \current control \system \current \control \system \current 
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
                                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
    Opens key:
 8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{add98944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{add98944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#ms_12tpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}

Opens key: HKLMNsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#ms ndiswanbh#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
 Opens~key: HKLMN~system\currentcontrolset\control\deviceclasses\ad498944-762f-11d0-8dcb-00c04fc3358c\} \\ \#?\#root\#ms\_ndiswanipv6\#0000\#\{ad498944-762f-11d0-8dcb-00c04fc3358c\}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Opens key:
 8dcb-00c04fc3358c}\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#ms_pptpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}

Opens key: HKLMNsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#ms sstpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#system#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
 8dcb-00c04fc3358c}
 Opens key:
82e6-71a87abac361}
                                                     HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c0382e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{cac88484-
                                                    7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-/ɔiɔ-4cuɔ 82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{cac88484-
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{cac88484
 7515-4c03-82e6-71a87abac361}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
   Opens key:
 82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}
 Opens key: HKLM\system\currentcontrolset\control\devicelasses\{cac88484-7515-4c03-82e6-71a87abac361}\\##?#root#ms_agilevpnminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\##?#root#ms_l2tpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLMI-xystem\currentcontrolset\control\deviceclasses\(\cac88484-7515-4c03-82e6-71a87abac361\)\#?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
    Opens key
 82e6-71a87abac361}\##?#root#ms_ndiswanip#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#root#ms_ndiswanipv6#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
 Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\#?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}\
 Opens key: HKLMN System\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\##?#root#ms_sstpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
```

```
82e6-71a87abac361}
Opens key:
ac88-96b894c191e2}
                                                          Opens key:
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
 ac88-96b894c191e2}\##?#
                                                       acpi#pnp0c0a#0#{e849804e-c719-43d8-ac88-96b894c191e2}
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
   Opens key:
bcaa-942b18988098}
   Opens key:
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
bcaa-942b18988098}\##?#usb#root_hub#48152cc75280#ted8cf6b1-62d5-4597-bcaa-942b18988098}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\(ed8cf6b1-62d5-4597-bcaa-942b18988098\)
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{ed8cf6b1-bcaa-942b18988098}\##?#usb#root_hub#4&22939226&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
\label{eq:open-sey} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{de8cf6b1-62d5-4597-bcaa-942b18988098}\
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
   Opens key
bcaa-942b18988098}\##?#usb#root_hub20#4&305beb51&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906hed83
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-
8815-00a0c906bed8}\##?#usb#root_hub#4&13571ab5&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
                                                          Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens kev:
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&24693ec3&0#{f18a0e88-c30c-11dd-8815-00a0c906bed8}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11dd-
8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub20#4&211f73e0&0#\\f18a0e88-c30c-11d0-8815-00a0c906bed8\
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\\ff18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub20#4&305beb51&0#\\ff18a0e88-c30c-11d0-8815-00a0c906bed8\\
    Opens kev:
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
olset\enum\umb\umb\1&841921d&0&printerbusenumerator
HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
    Opens key
08002be10318}
    Opens key:
                                                          HKLM\system\currentcontrolset\services\umbus
    Opens key
                                                          HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7
                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
    Onens key
Opens key:

HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllencodepublickeyandparameters
                                                          HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodepublickevandparameters
Opens key:
0\cryptdllencodeobjectex
                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
                                                         HKLM\software\microsoft\crvptography\oid\encodingtype
 1\cryptdllencodeobjectex
                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
    Opens key
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.1
                                                          HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.12
                                                         {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.2
                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
Opens key: httl://doi.org/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1001/wai-tuing/10.1
 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.4
                                                          HKLM\software\microsoft\windows\currentversion\setup
    Opens key:
    Opens kev:
                                                          HKLM\system\currentcontrolset\control\print
    Opens key:
                                                          HKCR\clsid
                                                          HKLM\software\policies\microsoft\windows nt\printers
    Opens key:
                                                         HKLM\system\currentcontrolset\services\lanmanworkstation\pa
HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
    Opens key:
                                                                                                                                                                   workstation\narameters
    Opens key:
    Opens key:
                                                          HKCR\appid\vssvc.exe
    Opens key:
                                                          HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\treatas
    Opens key:
    Opens key:
Opens key:
                                                          HKCR\clsid\\e579ab5f-1cc4-44b4-bed9-de0991ff0623\progid
HKCR\clsid\\e579ab5f-1cc4-44b4-bed9-de0991ff0623\\inprocserver32
    Opens key:
                                                          HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
    Opens key:
                                                         HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
    Opens key:
    Opens key:
Opens key:
                                                          \label{local-equation} $$HKCR\clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} $$ HKCR\clsid_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} \operatorname{local-equation} $$ HKCR_{clsid}_{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f} $$ here. $$ 
    Opens key:
                                                          HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprocserver32
    Opens key:
                                                          HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler32
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler
    Opens key:
    Opens key:
Opens key:
                                                          HKLM\system\currentcontrolset\services\vss\settings
    Opens key:
                                                          HKLM\system\currentcontrolset\services\vss\diag\registry writer
    Opens key:
                                                          HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}

HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
    Opens key:
                                                          HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32
    Opens key:
    Opens key:
    Opens kev
                                                          HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
    Opens key:
                                                          HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
    Opens key:
                                                          HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\progid
    Opens key:
    Opens key:
    Opens key
                                                          HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
                                                          HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
    Opens key:
    Opens key:
                                                         HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32
    Opens key:
    Opens key:
    Opens key
                                                          HKCR\clsid\{64h8f404-a4ae-11d1-h7h6-00c04fh926af}
    Opens key:
                                                          HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
    Opens kev:
                                                          HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\progid
                                                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
    Opens key:
    Opens key:
    Opens key
                                                          HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler
                                                          HKCR\cls10\\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\banker\bank
    Opens key:
    Opens key:
                                                          HKCR\interface\{00000100-0000-0000-c000-000000000046}
```

```
Opens key:
                                       HKCR\interface\{00000100-0000-0000-c000-00000000046}\proxystubclsid32
                                       HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}
HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
   Opens key:
   Opens key:
  Opens key:
                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
   Opens key:
                                      HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid
  Opens key:
                                      HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32
HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler32
   Opens key:
   Opens key:
  Opens key
                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler
                                      Opens key:
  Opens key:
                                      HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
HKLM\system\currentcontrolset\services\vss\diag\sar writer
   Opens key:
   Opens key:
  Opens key
                                       {\tt HKLM \corp} {\tt kklm \corp} {\tt corp} {\tt optimization}
writer
  Opens key:
                                       HKCR\interface\{0000000c-0000-0000-c000-000000000046}
                                      HKCR\interface\{0000000c-0000-0000-000000000046\\proxystubclsid32
HKLM\software\microsoft\windows nt\currentversion\svchost\wersvcgroup
   Opens key:
   Opens key:
   Opens key:
                                      HKLM\system\currentcontrolset\services\wersvc
HKLM\system\currentcontrolset\services\wersvc\parameters
   Opens key:
  Opens key:
                                       HKLM\software\microsoft\windows\windows error reporting
   Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\svchost\imgsvc
                                       HKLM\system\currentcontrolset\services\stisvc
  Opens key:
  Opens key:
                                      HKLM\system\currentcontrolset\services\stisvc\parameters HKLM\system\currentcontrolset\control\stillimage\trace
  Opens key:
                                       HKLM\svstem\currentcontrolset\control\stillimage\trace\wiaservc.dll
                                      HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
   Opens key:
  Opens key:
  Opens key:
                                      \label{thm:hkkcnclsid} $$HKCR\clsid{a1f4e726-8cf1-11d1-bf92-0060081ed811} \operatorname{hkkcnclsid}{a1f4e726-8cf1-11d1-bf92-0060081ed811} \operatorname{hkkcnclsid}{a1f4e726-8cf1-11d1-bf92-0060081ed811}
  Opens key:
                                       HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprocserver32
                                      HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler32
HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler
   Opens key:
  Opens key:
  Opens key:
                                      HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\treatas
  Opens key:
                                       HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\progid
                                      HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprocserver32
HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler32
   Opens key:
  Opens key:
  Opens key:
                                      HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler
HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
  Opens key:
                                       HKLM\svstem\currentcontrolset\control\stillimage\fakedevices
                                       HKLM\system\currentcontrolset\control\stillimage\mscdevicelist
   Opens key:
   Opens key:
                                       HKLM\system\currentcontrolset\control\stillimage
   Opens key:
                                      HKLM\system\currentcontrolset\control\stillimage\events
HKLM\system\currentcontrolset\control\stillimage\events
   Opens key:
  Opens kev:
HKLM\system\currentcontrol\set\control\stillimage\events\connected\{38f8a702-36bb-4a68-80e6d4966b9bb718}
  Opens key:
                                      Opens key:
  Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a3
                                       {\tt HKLM \ } system \verb|\ current control \verb|\ stillimage \verb|\ events \verb|\ faximage \verb|\ }
  Opens key:
  Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
  Opens key:
                                       HKLM\system\currentcontrolset\control\stillimage\events\printimage
   Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
   Opens key:
                                       HKLM\system\currentcontrolset\control\stillimage\events\scanbutton
  Opens kev:
HKLMNsystem \current control set \control \stillimage \events \scan but ton \{38f8a702-36bb-4a68-80e6-d4966b9b718\}
783ce7a92f22}
   Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}
                                       HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent
  Opens key:
   Opens key:
                                      HKLM\system\currentcontrolset\control\stillimage\serversettings
HKLM\system\currentcontrolset\services\nativewifip
   Opens key:
  Opens kev:
                                       HKLM\svstem\currentcontrolset\services\nativewifip\enum
   Opens key:
                                      HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
  Opens key:
Opens key:
0000f8753ed1}
                                       Opens key
                                       HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
08002be10318}
                                       HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
  Opens key:
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
Opens key: HKLM\system\currentcontrolset\services\nativewifip\parameters
   Opens kev
                                       HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
                                       HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000
   Opens key:
                                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens key
Opens key:

08002be10318}\0005\linkage

Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
                                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage
  Opens key:
Opens key:
                                      HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage
   Opens key:
HKLM\system\currentcontrolset\enum\pci\ven 8086&dey 100e&subsys 001e8086&rey 02\3&267a616a&0&18
Opens key: HI 08002be10318}\0007\linkage
                                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens key:
                                       HKIM\system\currentcontrolset\services\ndisuio\enum
   Opens key:
                                       HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000
                                       HKLM\svstem\currentcontrolset\enum\root\ms sstpminiport\0000
  Opens key:
   Opens ke
                                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
  Opens key:
                                      HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key
08002be10318}\0003\linkage
                                      HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens key:
  Opens key
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage
```

```
Opens key:
                                             HKLM\svstem\currentcontrolset\enum\root\ms agilevpnminiport\0000
Opens key: HI 08002be10318}\0001\linkage
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Opens key:
                                             HKLM\svstem\currentcontrolset\enum\root\*teredo\0000
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
08002be10318}\0011\linkage
                                             HKLM\system\currentcontrolset\enum\root\*isatap\0000
  Opens key:
                                             Opens key
08002be10318}\0009\linkage
  Opens key:
                                              ,
HKLM\system\currentcontrolset\control\diagnostics\performance
  Opens key:
                                             HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger
                                             HKLM\system\currentcontrolset\control\session
  Queries value:
manager[cwdillegalindllsearch]
  Queries value: HKLM\:
                                              HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
                                             HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Oueries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                             HKCU\control panel\desktop[preferreduilanguages]
HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
   Queries value
  Oueries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
HKLM\software\microsoft\rpc[maxrpcsize]
   Oueries value:
   Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
                                             HKLM\system\setup[oobeinprogress]
   Queries value:
Queries value:
                                             HKLM\system\setup[systemsetupinprogress]
HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
                                             HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:
Queries value:
                                             \label{thm:local-problem} HKLM\software\microsoft\windows nt\currentversion\compatibility32[alg]\\ HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]\\
  Oueries value:
                                             HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:
Queries value:
                                             HKLM\software\microsoft\ole[pageallocatorusesystemheap]
HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Oueries value:
                                             HKLM\software\microsoft\com3[com+enabled]
   Queries value:
                                              HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
                                             HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
   Oueries value:
   Queries value:
                                             HKLM\software\microsoft\ole[defaultaccesspermission]
HKLM\system\currentcontrol\set\control\lsa[everyoneincludesanonymous]
   Queries value:
  Oueries value:
                                             HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                                             {\tt HKLM} \verb|\software\microsoft\cryptography\defaults\provider\microsoft\ strong
   Oueries value
cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:
                                             {\tt HKLM \ } system \verb| current control \verb| sa \verb| fips algorithm policy [enabled] \\
   Oueries value:
                                             HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicv]
   Queries value:
                                             HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
   Queries value:
\label{local-problem} \begin{split} & HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography[privkeycachepurgeintervalseconds] \\ & Queries value: & HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography[privatekeylifetimeseconds] \end{split}
                                             HKLM\software\microsoft\cryptography[machineguid]
HKCR\interface\{0000134-0000-0000-0000-0000000046}\proxystubclsid32[]
HKLM\software\microsoft\rpc\extensions[ndroleextdll]
   Oueries value:
   Queries value
  Queries value:
   Oueries value
                                             HKLM\software\microsoft\rpc\extensions[remoterpcdll]
                                              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[bca9f854]
   Queries value
   Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
\label{local-prop} HKLM\software\microsoft\sqmclient\swindows\disabledsessions[globalsession] \\ Queries\ value: HKLM\software\microsoft\ole[maxsxshashcount] \\
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\compatibilitv32[msdtc]
   Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_misc]
HKLM\software\microsoft\msdtc\tracing\sources[trace_cm]
  Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
HKLM\software\microsoft\msdtc\tracing\sources[trace_svc]
   Oueries value
   Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_gateway]
HKLM\software\microsoft\msdtc\tracing\sources[trace_ui]
HKLM\software\microsoft\msdtc\tracing\sources[trace_contact]
   Oueries value:
   Queries value:
  Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
HKLM\software\microsoft\msdtc\tracing\sources[trace_cluster]
   Oueries value:
   Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_resource]
HKLM\software\microsoft\msdtc\tracing\sources[trace_tip]
HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
   Oueries value:
   Queries value:
  Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_log]
HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
   Oueries value:
   Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
HKLM\software\microsoft\msdtc\tracing\sources[trace_ktmrm]
   Oueries value:
   Queries value:
  Queries value:
  Queries value:
Queries value:
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_vssbackup]
HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon]
                                             HKLM\software\microsoft\msdtc\tracing\sources[trace_tml]
HKLM\software\microsoft\msdtc\tracing\sources[trace_tml]
HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
HKLM\software\microsoft\msdtc\tracing\output[tracefilepath]
HKLM\software\microsoft\msdtc\tracing\output[memorybuffersize]
HKLM\software\microsoft\msdtc\tracing\output[debugoutenabled]
   Oueries value:
   Queries value
  Oueries value:
   Queries value:
   Queries value:
   Oueries value:
                                              HKLM\software\microsoft\msdtc[noparallellogflushnotification]
HKLM\software\microsoft\msdtc[snapshotprefertransactionstimeoutduringbackup]
                                             HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
HKLM\software\microsoft\windows
   Queries value:
  Queries value
\label{thm:currentversion} $$ nt\currentversion\tracing\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSdfware}\mbox{\cite{MSd
                                             HKLM\software\microsoft\msdtc[sysprepinprogress]
HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\description[]
  Oueries value:
   Queries value:
   Queries value:
   Oueries value
                                             HKCR\cid local\81a3a129-619d-4d5f-a782-28d960ea489d\description[]
                                             HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5\description[]
HKCR\cid.local\8b9b59d3-8bb9-4d71-af93-3faf363251c9\description[]
   Queries value:
  Oueries value:
                                             HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\description[]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid[]
   Queries value:
   Queries value:
   Oueries value
                                              HKCR\cid local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\bost[]
   Queries value:
                                              HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\clsid[]
  Oueries value:
                                              HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
                                             HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\protocol[]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\endpoint[]
   Oueries value:
   Queries value:
   Oueries value
                                             HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
                                           erties\log\size[]
782ab52d45ed\customprop
```

Oueries value: HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]

HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib] Oueries value

```
Oueries value:
                                                      HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
                                                      HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
    Oueries value
   Queries value:
                                                      Oueries value:
   Queries value
   Oueries value:
                                                      HKLM\software\microsoft\msdtc\securitv[networkdtcaccessadmin]
                                                      HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
   Queries value:
   Queries value:
                                                      \label{thm:hklm-software-microsoft-msdtc-security} HKLM \software-microsoft-msdtc[allowonlysecurerpccalls]
   Oueries value
   Queries value
   Oueries value:
                                                       HKLM\software\microsoft\msdtc\securitv[xatransactions]
                                                      HKLM\software\microsoft\msdtc\security[lutransactions]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
   Queries value:
   Queries value:
782ab52d45ed\customprop
                                                   erties\log\path[]
HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-
Queries value:
8bd7-da8f1a74051a]
   Queries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
   Oueries value
                                                      HKLM\software\microsoft\window
nt\currentversion\tracing\msdtc\loggingoptions[maxbuffers]
   Oueries value:
                                                      HKLM\software\microsoft\window
\verb|nt\currentversion| tracing \verb|msdtc| logging options[minbuffers]|
                                                      HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\tracing\msdtc\loggingoptions[buffersize]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxfilesize]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[bias]
Queries value: HKLM\system\currentcontrolset\control\timezoneinformation[standardname]
   Queries value:
Queries value:
                                                      \label{thm:local_hammon_hammon} HKLM \system \current control \control \timezone in formation [standard bias] \\ HKLM \system \current control \control \timezone \cine formation [standard start]]
   Oueries value:
                                                      HKLM\system\currentcontrolset\control\timezoneinformation[davlightname]
     Queries value:
                                                       HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
                                                      HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]
   Queries value:
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[uniqueid]
   Oueries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[active]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[level]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[controlflags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[uniqueid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
   Oueries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
   Oueries value:
                                                      HKLM\software\microsoft\windows
\label{lem:ntcurrent} $$ nt\currentversion\tracing\mbox{\sc Nmodules}\transaction\_transitions[controlflags] $$ Queries\ value: $$ HKLM\system\currentcontrolset\control\mbox{\sc Nmodules}\transaction\_transitions[controlflags] $$ Added-transaction\_transitions[controlflags] $$ Output $$ (1.5) $$ and $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) $$ (1.5) 
af58-73e332dcac8d1
   Queries value:
                                                       HKLM\software\microsoft\msdtc[dtcmaxsessions]
   Oueries value:
                                                      HKLM\software\microsoft\msdtc[donotgoidle]
  Queries value:
Queries value:
                                                      HKLM\software\microsoft\msdtc[disabletippassthrucheck]
HKLM\software\microsoft\msdtc[mincheckpointinterval]
   Oueries value
                                                      HKLM\software\microsoft\msdtc[maxcheckpointinterval]
   Queries value:
                                                       HKLM\software\microsoft\msdtc[waitforallxabranchprepares]
   Oueries value:
                                                      HKLM\software\microsoft\msdtc\securitv[snapshotsecuritydisabled]
   Queries value:
                                                      HKLM\software\microsoft\msdtc[servertcpport]
HKLM\software\microsoft\windows nt\currentversion[currentversion]
   Queries value:
                                                      HKLM\software\microsoft\msdtc[cmcancelrpcafter]
HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
   Oueries value
   Queries value:
   Oueries value:
                                                       HKLM\software\microsoft\msdtc[cmmaxidlepings]
   Queries value:
                                                      HKLM\software\microsoft\msdtc[cmpingfreqsecs]
HKLM\software\microsoft\msdtc[cmverbose]
   Queries value:
                                                      HKLM\software\microsoft\msdtc[rpcqoscapabilities]
HKLM\software\microsoft\msdtc[rpcqosidentity]
   Oueries value
   Queries value:
                                                      HKLM\software\microsoft\msdtc[rpcauthnsvc]
HKLM\software\microsoft\msdtc[numcccimhistoryentries]
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\svcid[]
   Oueries value:
   Queries value:
   Queries value:
   Oueries value
                                                       HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\host[]
   Queries value:
                                                       HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\clsid[]
   Oueries value:
                                                       HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
    Queries value:
                                                      HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\protocol[]
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\endpoint[]
   Queries value:
                                                      HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Oueries value:
   Queries value:
   Oueries value:
                                                       HKLM\software\microsoft\msdtc[notracking]
                                                       HKLM\software\microsoft\rpc\securityservice[9]
    Queries value
   Queries value
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedl1]
Queries value:
HKLM \simeq Current control \simeq Control \simeq Current con
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
   Queries value:
Queries value:
                                                      HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dl1[name] HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dl1[comment]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
                                                      HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
   Oueries value:
                                                      HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version] HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
   Queries value:
   Queries value
   Oueries value
Oueries value:
HKLMNsystem\currentcontrolset\control\lsa\accessproviders[martaextension]

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
                                                      Oueries value:
   Queries value:
   Oueries value:
                                                      HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
                                                      HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\host[]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\clsid[]
   Queries value:
   Queries value:
                                                      \label{local_hammon_mutex_timeout} HKLM\software\microsoft\mbox{\sc } hared\_memory\_mutex\_timeout] \\ HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider[] \\
   Oueries value
   Queries value:
                                                       HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol[]
   Oueries value:
                                                      HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\endpoint[]
HKLM\software\microsoft\msdtc[overridetiphostname]
   Queries value:
   Queries value:
                                                       HKCR\cid local\81a3a129-619d-4d5f-a782-28d960ea489d\svcid[]
   Oueries value
                                                      HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\host[]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\clsid[]
   Queries value:
   Oueries value:
                                                      HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[] HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\protocol[]
   Queries value:
   Queries value:
   Oueries value
                                                       HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\endpoint[]
   Queries value
                                                       HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
   Oueries value:
                                                       HKLM\software\microsoft\msdtc[xatmmaxwarmrecovervinterval]
                                                       HKLM\software\microsoft\msdtc[transactionbridge]
```

```
Oueries value:
                                           HKLM\software\microsoft\msdtc[logwarnenabled]
                                           HKLM\software\microsoft\msdtc[suppressduplicateduration]
HKLM\software\microsoft\msdtc[suppressduplicateduration]
HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9c4d}\progid[]
   Queries value
   Queries value:
   Oueries value
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
   Queries value
  Oueries value
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-
                                          rer32[inprocserver32]
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
b913c40c9cd4}\inprocser
  Queries value:
   Oueries value
                                           HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocser
                                          er32[threadingmodel]
  Oueries value
                                           HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                                           HKLM\software\microsoft\msdtc[supportns]
HKLM\software\microsoft\windows
   Queries value
  Queries value:
nt\currentversion\compatibility32[ui0detect]
Queries value: HKU\.default\control panel\desktop[preferreduilanguages]
  Oueries value
                                           HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable] Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
  Oueries value:
                                           HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                           HKLM\system\currentcontrolset\control\nls\language groups[1] HKLM\software\microsoft\windows
   Queries value:
  Queries value:
nt\currentversion\langu
                                         agepack\datastore_v1.0[disable]
HKLM\software\microsoft\window
  Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: nt\currentversion\
                                        HKLM\software\microsoft\windows
uagepack\surrogatefallback[plane2]
  Oueries value:
                                           HKLM\software\microsoft\windows
nt\currentversion
                                    nguagepack\surrogatefallback[plane3]
                                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane7]
  Oueries value:
                                           HKLM\software\microsoft\windows
nt\currentversion
                                 anguagepack\surrogatefallback[plane8]
  Oueries value:
                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
\begin{tabular}{ll} nt`currentversion\languagepack\surrogatefallback[plane10]\\ Queries value: HKLM\software\microsoft\windows \end{tabular}
nt\currentversion\languagepack\surrogatefallback[plane111
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane12]
  Oueries value
                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Oueries value:
                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
\begin{tabular}{ll} nt`currentversion\languagepack\surrogatefallback[plane15]\\ Queries value: HKLM\software\microsoft\windows \end{tabular}
nt\currentversion\languagepack\surrogatefallback[plane161
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[localservicepeernet]
  Oueries value
                                           HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
   Queries value:
HKLM\svstem\currentcontrolset\services\p2pimsvc\parameters[servicemanifest]
   Queries value:
                                           HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain] HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\winlogon[userenvdebuglevel]

Queries value: HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
   Oueries value:
                                           HKLM\software\policies\microsoft\peernet[disabled]
   Queries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedllunloadonstop]
  Oueries value:
                                           HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll]
   Queries value:
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]
   Queries value:
                                           HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
   Queries value
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog9[serial\_access\_num]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Oueries value
Oueries value
Oueries value
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000005packedcatalogiteml
   Queries value
Oueries value
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[packedcatalogitem]
  Oueries value
Queries value
\label{local-proposed-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000010\packedcatalogitem]
   Queries value
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\spaces\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parame
  Oueries value
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000012[packedcatalogitem]
  Oueries value
Queries value:
\label{local-parameters-protocol} HKLM\system \colors a log_entries $$00000000014[packed catalogitem]$ Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000016\packedcatalogitem]
   Oueries value
Oueries value:
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\spaces\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parame
   Oueries value:
\label{local-parameters} HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog 5 \[serial\_access\_num] \]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5[num catalog entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001flibrarypath]
   Queries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\commont{0}0000000001[providerid]
   Oueries value:
Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\namespace] Queries\value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[enabled]
   Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
   Oueries value
HKL\\ M\system\current control set\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\colored by the control set and the control set
   Oueries value:
Queries value:
HKLM \label{lem:hklm} HkLM \label{lem:hklm} HkLM \label{lem:hklm} With the lem \label{lem:hklm} With the lem \label{lem:hklm} With the lem \label{lem:hklm} With the lem \label{lem:hklm} HkLM \label{lem:hklm} With the lem \label{lem:hklm} HkLM \label{lem:hklm} With the lem \la
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000002[displaystring]
   Queries value
Queries value:
Oueries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
HKL\\ M\system\current control set\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\space\sp
   Queries value:
Oueries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 000000000003 [library path]
   Oueries value:
HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog5 \catalog\_entries \names 
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003fproviderid1
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003faddressfamilv1
   Queries value:
Oueries value
HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace\_catalog \\ 5 \\ catalog\_entries \\ 0000000000003 \\ [enabled]
   Oueries value:
Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 000000000003[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003fproviderinfol
   Queries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\common000000004[displaystring]
   Oueries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000004fsupportednamespace1
   Queries value:
HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace\_catalog \\ 5 \\ catalog\_entries \\ 00000000000004 \\ [enabled]
   Oueries value
Oueries value:
Queries value:
Oueries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 000000000005 [library path]
Oueries value:
Oueries value:
Oueries value:
Queries value:
HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace\_catalog \\ 5 \\ catalog\_entries \\ 00000000000005 \\ [enabled]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005fversion1
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[storesserviceclassinfo]
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
  Oueries value:
HKL\\ M\system\current control set\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath]
   Queries value:
\label{local-parameters} HKLM \system \current controlset \services \winsock 2 \parameters \names pace\_catalog5 \catalog\_entries \00000000000006 \[displaystring] \queries \value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006fproviderid1
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
   Oueries value
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\space]
  Oueries value:
Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000006[version] \\ Queries\value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[storesserviceclassinfo]
   Oueries value
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006fproviderinfol
    Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Oueries value:
                                                  HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Oueries 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
   Oueries value:
                                                 HKLM\svstem\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
    Queries value:
\label{lem:hkkm} Hkklm\system\corrent control set\services\tcpip6\parameters\winsock[minsockaddrlength] Queries\ value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
   Oueries value
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
   Oueries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
    Queries value
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
   Queries value:
c19ce8a73253}[domain]
   Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253\}[dhcpdomain]
   Oueries value:
c19ce8a73253}[dhcpv6domain]
806e6f6e6963}[enabledhcp]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
Queries value:
806e6f6e6963}[registeradaptername]
   Oueries value:
HKLMNsystem \current control set \services \tcpip\parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [domain]
   Oueries value:
806e6f6e6963}[dhcpdomain]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
                                                  HKLM\software\microsoft\sqmclient[machineid]
   Queries value:
   Oueries value
                                                  HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%11/8[seedserver]
                                                  HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
   Oueries value:
Queries value: httm://doi.org/10.1001/j.mklocal_ff00::%11/56[disablemulticastpublish]
Queries value: httm://doi.org/10.1001/j.mklocal_ff00::%11/56[disablemulticastpublish]
Queries value: httm://doi.org/10.1001/j.mklocal_ff00::%11/56[disablemulticastpublish]
linklocal\linklocal_ff00::%11/8[disablemulticastsearch]
Queries value: HKLM\software\mic
linklocal\linklocal_ff00::%11/8[disabled]
                                                  HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
Queries value: HKLM\software\nicrosoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[searchonly]
   Oueries value
                                                 HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6
linklocal\linklocal_ff00::%11/8[mincpalifetime]
   Oueries value:
HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[category]
   Oueries value:
a03a-e3ef65729f3d}[name1
    Queries value
a03a-e3ef65729f3d}[parentfolder]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\f3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[description]
   Queries value:
a03a-e3ef65729f3d}[relativepath]
   Oueries value:
\label{lem:condition} White the description of the description of the descriptions of the descriptions of the description of 
Queries\ value: \\ HKLM\ value: \\ H
a03a-e3ef65729f3d}[infotip]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localizedname]
   Queries value:
a03a-e3ef65729f3d}[icon]
   Oueries value:
a03a-e3ef65729f3d}[security]
   Oueries value:
 a03a-e3ef65729f3d}[streamresource]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresourcetype]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localredirectonly]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[roamable]
   Oueries value:
a03a-e3ef65729f3d}[precreate]
   Oueries value:
 HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[stream]
   Oueries value:
```

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[publishexpandedpath]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[attributes]

Oueries value:

 $HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[foldertypeid]$ 

Oueries value:

ad3a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

Oueries value HKIM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public] HKLM\software\microsoft\windows nt\currentversion\profilelist[default] HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: 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)] HKLM\software\microsoft\windows\currentversion[programw6432dir]
HKLM\software\microsoft\windows\currentversion[commonw6432dir] Queries value: Queries value: Oueries value HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19[profileimagepath]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local appdata]

HKCU\control panel\international[localename] Queries value:

Oueries value

 $\label{thm:continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folds \folds$ 9afe-ea3317b67173}[category]

 $HKLM \label{eq:hkkkk} Which is the standard of the standard$ 9afe-ea3317b67173}[name] Queries value:

9afe-ea3317b67173}[parentfolder]

Queries value:

 $\label{thm:local_hklm} \begin{tabular}{ll} HKLM \software \mbox{$microsoft} \windows \current version \explorer \folder descriptions \folder \current version \explorer \folder \current \curr$ 9afe-ea3317b67173}[description]

Oueries value:

9afe-ea3317b67173}[relativepath]

Oueries value:

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

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

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

Oueries value:

 $\label{thm:local_hklm} \begin{tabular}{ll} HKLM \software \mbox{$microsoft} \windows \current version \explorer \folder descriptions \folder \current version \explorer \folder \current \curr$ 9afe-ea3317b67173}[icon]

Oueries value:

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

Queries value:

 $HKLM \label{eq:hkkkk} Which is the standard of the standard$ 9afe-ea3317b67173}[streamresource]

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

Queries value:

9afe-ea3317b67173}[localredirectonly]

Oueries value:

 $HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [roamable]$ 

Oueries value:  $\label{thm:continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} \end{4.5} $$ 66c858f-0e22-4760-1000 \cite{1.5} \cite{1.5} \end{4.5} $$ 1000 \cite{1.5} \cite{1.5}$ 

9afe-ea3317b67173}[precreate]

 $HKLM \label{eq:hkkkk} Which is the standard of the standard$ 

9afe-ea3317b67173}[stream] Queries value:

 $HKLM \label{eq:hkkkk} Which is the standard of the standard$ 

9afe-ea3317b67173}[publishexpandedpath]

Queries value:

9afe-ea3317b67173}[attributes]

Oueries value:

 $HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{5e6c858f-0e22-4760-9afe-ea3317b67173\}[foldertypeid]$ 

Queries value:

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

HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

HKLM\software\microsoft\cryptography\defaults\provider types\type Oueries value: 012[name]

Queries value:  ${\tt HKLM} \verb|\software\microsoft\cryptography\defaults\provider\microsoft\ rsa\\$ 

schannel cryptographic provider[image path]

Queries value

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\\\ 62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[category]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[name] Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[parentfolder]

Oueries value: 

a9dd-070d1d495d97}[description] Oueries value:

a9dd-070d1d495d97}[relativepath]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\\\ 62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[parsingname]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[infotip]

Oueries value: a9dd-070d1d495d97}[localizedname] Oueries value: a9dd-070d1d495d97}[icon] Queries value: a9dd-070d1d495d97}[securitv] a9dd-070d1d495d97}[streamresource] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[streamresourcetype]

Oueries value: a9dd-070d1d495d97}[localredirectonly]

Oueries value: a9dd-070d1d495d97}[roamable]

Oueries value:  $HKLM \label{eq:hkkkk} Which is the statement of the sta$ a9dd-070d1d495d97}[precreate]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3a9dd-070d1d495d97}[stream]

Queries value: a9dd-070d1d495d97}[publishexpandedpath] Oueries value:

a9dd-070d1d495d97}[attributes] Oueries value:

 $\label{thm:local-bound} \begin{tabular}{ll} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\folder$ a9dd-070d1d495d97}[foldertypeid]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\\\ 62ab5d82-fdc1-4dc3a9dd-070d1d495d97}[initfolderhandler]

Queries value: HKLM\software\policies\microsoft\cryptography[forcekeyprotection]

Oueries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7[name] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\65a9a6cf-64\text{843e-32c86e1ba19f}\\##?#umb#umb#1&841921d&0&printerbusenumerator#\\65a9a6cf-64cd-480b-843e-HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-32c86e1ba19f}[deviceinstance]

HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-Queries value: 843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e 32c86e1ba19f}\#\control[linked]

HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-Oueries value: 843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\control[referencecount]

Oueries value HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}[default] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-Oueries value:

b082-00a0c91efb8b\\##? #pci#ven\_1000&dev\_0054&subsys\_1f091028&rev\_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-

00a0c91efb8b}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}\##?#pci#ven\_1000&dev\_0054&subsys\_1f091028&rev\_01#5&6373acf&0&400008#{2accfe60-

c130-11d2-b082-00a0c91efb8b}{deviceinstance}

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-

b082-00a0c91efb8b}\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082

00a0c91efb8b}[deviceinstance] Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&0#{2accfe60-c130-11d2-b082-

00a0c91efb8b}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-Oueries value b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&1#{2accfe60-c130-11d2-b082-

00a0c91efb8b}[deviceinstance] Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\2accfe60-c130-11d2-b082-00a0c91efb8b\\#?\pciide\devidechannel\devidechann

00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{2acb082-00a0c91efb8b}\\##?\pciide\pidechannel\pi4&2f42c713&0&0\pi\{2accfe60-c130-11d2-b082-00a0c91efb8b}\\\##\prox \pi \text{Control}\text{Verification} \text{Verification} \tex

00a0c91efb8b}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-Queries value: b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&1#{2accfe60-c130-11d2-b082-

00a0c91efb8b}[deviceinstance] Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-84ae-d30803bae505}[default]

HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-Queries value: 84ae-d30803bae505}\##?#root#vdrvroot#0000#{2e34d650-5819-42ca-84ae-d30803bae505}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1bc8c-00a0c91405dd}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#acpi#pnp0f03#4&1d401fb5&0#{378de44c-56ef-11d1-bc8c-

00a0c91405dd}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-1bc8c-00a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&col02#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-OdaoC91405d4} [deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-

bc8c-00a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&col02#6&1e20eb37&0&0001#{378de44c-56ef-11d1-bc8c 00a0c91405dd}[deviceinstance]

HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-Oueries value: bc8c-00a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&co103#6&1c83c2e&0&0002#{378de44c-56ef-11d1-bc8c 00a0c91405dd}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\\ 378de44c-56ef-11d1-bc8c-00a0c91405dd\\\##?\#hid\#vid\_14dd\\\particlespid\_1005\\ col03\#681e20eb37\\\ 080002\#\\\ 378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance]

Queries value: HKLMsystem\currentcontrolset\control\deviceclasses\{378de44c-56ef-11dbc8c-00a0c91405dd}\#?#root#rdp\_mou#0000#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[default]

HKI M\system\currentcontrolset\control\deviceclasses\{3ahf6f2d-71c4-462a-Oueries value: 8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27c8&subsys\_01e61028&rev\_01#3&2411e6fe&0&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27c8&subsys\_01e61028&rev\_01#3&2411e6fe&1&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]

HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven\_8086&dev\_27c9&subsys\_01e61028&rev\_01#3&2411e6fe&0&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]

```
Oueries value:
                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&1&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]
71c4-462a-8a92-1e6861e6af27}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&1&ea#{3abf6f2d-
71c4-462a-8a92-1e6861e6af27}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&0&ef#{3abf6f2d-
71c4-462a-8a92-1e6861e6af277{[deviceinstance]}
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&1&ef#{3abf6f2d-
71c4-462a-8a92-1e6861e6af27}[deviceinstance]
   Oueries value:
                                           HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662-
b732-99a6111edc0b}[default]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-
  Queries value:
a5d6-28db04c10000}[default]
                                           HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-
a5d6-28db04c10000}\##?#root#system#0000#{4747b320-62ce-11cf-a5d6-28db04c10000}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-
   Queries value
be5e-00a0c9062857}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e-
00a0c9062857}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-
be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&1#{4afa3d53-74a7-11d0-be5e-
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\be5e-00a0c9062857\\#?#acpi#fixedbutton#2&daba3ff&2#{4afa3d53-74a7-11d0-be5e-be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&2#
Queries Value: McLm\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-00111100030}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}
001111000030}[deviceinstance]
                                           HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
  Queries value:
88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&0000#{4d1e55b2-f16f-11cf-88cb-
001111000030}[deviceinstance]
  Oueries value:
                                          HKLM\svstem\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&1c83c2e&0&0001#{4d1e55b2-f16f-11cf-88cb-
001111000030}[deviceinstance]
Oueries value: HKLMsystem\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-00111100030}\#;?#hid#vid_14dd&pid_1005&col02#6&1e20eb37&0&0001#{4d1e55b2-f16f-11cf-88cb-
001111000030}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&1c83c2e&0&0002#{4d1e55b2-f16f-11cf-88cb
001111000030}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&1e20eb37&0&0002#{4d1e55b2-f16f-11cf-88cb-
001111000030}[deviceinstance]
                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
   Oueries value
94f2-00a0c91efb8b}[default]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
  Queries value:
94f2-00a0c91efb8b}\##?
#ide#diskhitachi_
                                                                                     __3.5.1.9_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
Queries value:
94f2-00a0c91efb8b}\##?
#ide#diskybox harddisk
                                                                                                     #5&394c0ad3&0&0 0 0#{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}[deviceinstance]
                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
  Oueries value:
Queries value.

94f2-00a0c91efb8b}\##?#scsi#disk8wen_dell&prod_virtual_disk#6&17b13437&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries \ value: \ HKLM\ system \ (current control set\ control\ device classes\ \{53f56307-b6bf-11d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&00000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_di
11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKl 94f2-00a0c91efb8b}[default]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
  Oueries value:
                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
t10n______#5&28836b8&0&0.0.0#{53f56308-b6bf-11d0-94f2-
Queries value: HKLM\system\cur
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
                                                       _1.0_
                                                                     #5&106af171&0&1.0.0#{53f56308-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
  Oueries value:
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                      ___1.0_____#5&394c0ad3&0&0.1.0#{53f56308-b6bf-11d0-94f2-
rom_
00a0c91efb8b}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value: HKL 94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolse
94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
                                           HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
t10n_____1.02__#5&28836b88&0&0.0.0#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                          HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Oueries value:
00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value: HKLM\system\cur
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                    ____1.0_____#5&106af171&0&1.0.0#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                           HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
   Oueries value
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                                      #5&394c0ad3&0&0 1 0#{53f5630d-b6bf-11d0-94f2-
                                                       1.0
rom
  Oueries value:
                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{69d250e0-6c18-11e3-b3bc-
806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries \ value: \\ HKLM\system \ (current control set\ (control \ device classes\ \{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\}\ ) \\ *** \ (45d-20a0c91efb8b) \ (
806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#?#storage#volume#\{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#0000000000000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
                                           HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#000000075343e000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
```

```
Oueries value:
                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\\ 53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\##?#storage#volume#\\\ 74a4ebdb-f4e7-11df-aef6-\\\ 806e6f6e6963\\\ #0000020d3a1e800#\\\ 53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\\\\ [deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963\\\00000000000020f3026800\\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\\deviceipstance\
Queries value: HKLM\system\currentcontrol\set\control\
94f2-00a0c91efb8b\\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
806e6f6e6963}#000000211262e800#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Oueries value:
94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-
806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\{e29ac6c3-7037-11de-816d-
806e6f6e6963\}\#00000000000000000000000\#\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\}[deviceinstance]\\ Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\}[deviceinstance]
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000000075343e0000#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?#storage#volume#{e29ac6c3-7037-11de-816d-806e6f6e6963}#0000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot1#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b\} \verb||#|| *|#storage#volumesnapshot|| *|harddiskvolumesnapshot|| 10 # \{53f5630d-b6bf-11d0-94f2-b6bf-11d0-94f2-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d
00a0c91efb8b}[deviceinstance]
00a0c91efb8b}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot2#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Queries value:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f5630d-b6bf-11d0-94f2
00a0c91efb8b}[deviceinstance]
                                   HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Oueries value:
Queries value.

94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot4#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
  Oueries value
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
00a0c91efb8b}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#yolumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}[deviceinstance]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value.

94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
  Oueries value
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
94f2-00a0c91efb8b}[default]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
  Oueries value:
94f2-00a0c91efb8b}\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
8Sbb-30ff1f953599}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&1fc3087&0&28f0#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
                                   HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
  Queries value:
85\dot{b}-30ff1f953599\} \\ \#?\#pci\#ven\_1002\&dev\_515e\&subsys\_01e61028\&rev\_02\#4\&2e5a831\dot{d}\&0\&28f0\#\{5b45201d-f2f2-4f3b-85bb-30ff1f953599\}[deviceinstance]
                                   HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
  Oueries value:
85bb-30ff1f953599}\##?#pci#ven_80ee&dev_beef&subsys_00000000&rev_00#3&267a616a&0&10#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}[default]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
  Oueries value:
843e-32c86e1ba19f}\##?#root#umbus#0000#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}[deviceinstance]
                                    Oueries value:
bcf7-00aa00b7b32a}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
Queries value: HK
a537-0000f8753ed1}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-a537-0000f8753ed1}\\##?#lptenum#microsoftrawport#5898f833e&0&lpt1#{811fc6a5-f728-11d0-a537-
0000f8753ed1}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#482abfaa3080&12345678&00802#{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2dcf5eab&0&12345678&06&05#{866519b5-3f07-4c97-
D7df-24C5d8a8ccb8}{deviceinstance}
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}\##?#display#default_monitor#582fab8e3980812345678806805#{866519b5-3f07-4c97-b7df-24c5d8a8ccb8}{deviceinstance}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Oueries value:
bc8c-00a0c91405dd}[default]
```

```
bc8c-00a0c91405dd}\##?#acpi#pnp0303#4&1d401fb5&0#{884b96c3-56ef-11d1-bc8c-
00a0c91405dd}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Oueries value
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co101#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c
00a0c91405dd}[deviceinstance]
00a0c91405dd}[deviceinstance]
Oueries value: HKLM system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\#;?#root#rdp_kbd#0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
af1f-0000f800845c}[default]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
  Oueries value:
af1f-0000f800845c}\##?#acpi#pnp0400#4&1d401fb5&0#{97f76ef0-f883-11d0-af1f-
0000f800845c}[deviceinstance]
   Queries value
                                     HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
359c-8bef029dbdd0}[default]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
  Oueries value:
359c-8bef029dbdd0}\##?#acpi#genuineintel_-_x86_family_6_model_15_
 intel(r) xeon(r) cpu
                                              __x3220__@_2.40ghz#_1#{97fadb10-4e33-40ae-359c-
8bef029dbdd0}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
  Queries value:
Queries value. 359c-8bef029dbdd0}\##?#acpi#genuineintel___x86_family_6_model_15__
_intel(r)_xeon(r)_cpu____x3220__@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-
8bef029dbdd0}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
   Queries value
Queries value: MFLMNsystem.currentcontrolset\Control\deviceclasses\ 359c-8bef029dbdd0}\#r?#acpi#genuineintel_-_x86_family_6_model_15_-
_intel(r)_xeon(r)_cpu____x3220_@_2.40ghz#_3#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
                                   HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
  Oueries value:
359c-8bef029dbdd0}\#r?#acpi#genuineintel_-_x86_family_6_model_15_-
_intel(r)_xeon(r)_cpu____x3220__@_2.40ghz#_4#{97fadb10-4e33-40ae-359c-8bef029dbdd0}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-
901f-00c04fb951ed}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34a9bc#{a5dcbf10-6530-11d2-901f-
00c04fb951ed}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Oueries value:
8dcb-00c04fc3358c}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{ad498944-
762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Oueries value:
Queries value: MrLMNsystem/currentcontrolset\control\deviceclasses\{add98944-762T-11d0 8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{add98944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad498944
762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\\ ad498944-762f-11d0-8dcb-00c04fc3358c\\\\ #?#root#*isatap#0000#\{ad498944-762f-11d0-8dcb-00c04fc3358c\\\\ [deviceinstance]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Oueries value:
8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
  Oueries value
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_l2tpminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
Oueries value: HKLM\system\currentcontrol\set\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#ms_ndiswanbh#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_ndiswanipv6#0000#{ad498944-762f-11d0-8dcb
00c04fc3358c}[deviceinstance]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c\} \verb|\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-10c04fc3358c}| \verb|\##:#root#ms_pppoeminiport#0000#| \verb|\##:#root#ms_pppoeminiport#00
00c04fc3358c}[deviceinstance]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_pptpminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\{ad498944-762f-11d0-8dcb-00c04fc3358c}\\##?\root\mis_sstpminiport\rightarroot\devided498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#system#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}|deviceinstance|
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\\#?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-
8dcb-00c04fc3358c}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{cac88484-
7515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{cac88484-
7515-4c03-82e6-71a87abac361}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Oueries value:
82e6-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{cac884847515-4c03-82e6-71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Oueries value:
82e6-71a87abac361}\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Oueries value:
82e6-71a87abac361}\##?#root#ms_agilevpnminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_l2tpminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
  Oueries value
                                     HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\##?\root\ms_n\diswanip\#0000\rangle(cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_ndiswanipv6#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
```

HKLM\svstem\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-

Oueries value:

```
Oueries value:
                                      HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}[deviceinstance]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\#?\root\mis_sstpminiport\rightarroot\deviceclasses\{cac88484-7515-4c03-82e6-
71a87ahac3613[deviceinstance]
//da/abd/soij/ueviteinstance;
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
ac88-96b894c191e2}[default]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{e849804e-c719-ac88-96b894c191e2}\##?#acpi#pnp0c0a#0#{e849804e-c719-43d8-ac88-96b894c191e2}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
  Queries value:
                                      HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
bcaa-942b18988098}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}\##?#usb#root_hub#4&152cc752&0#{ed8cf6b1-62d5-4597-bcaa-
942b18988098}[deviceinstance]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\ed8cf6b1-62d5-4597-bcaa-942b18988098\\#?#usb#root_hub#482293922680#\ed8cf6b1-62d5-4597-bcaa-
942b18988098}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\{ed8cf6b1-62d5-4597-bcaa-942b18988098\\\#?\#usb\#root_hub\#482a2237a3\\00e408cf6b1-62d5-4597-bcaa-
942b18988098}[deviceinstance]
942bio360030[[uevleta:is:HKLM\system\currentcontrolset\control\deviceclasses
| Gueries value: HKLM\system\currentcontrolset\control\deviceclasses
| bcaa-942b18988098}\##?#usb#root_hub20#4&305beb5180#{ed8cf6b1-62d5-4597-bcaa-
                                      HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
00a0c906bed8}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
  Queries value:
8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&22939226&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub#4824693ec3&0#\f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclass
8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-
                                      HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
00a0c906bed8}[deviceinstance]
                                      HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
  Queries value:
8815-00a0c906bed8}\##?#usb#root_hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
                                     HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
  Oueries value:
8815-00a0c906bed8}\##?#usb#root_hub20#4&211f73e0&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
  Oueries value
                                     HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub20#4&305beb51&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Oueries value: HKLM:system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\f18a0e
8815-00a0c906bed8\\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#\f18a0e88-c30c-11d0-8815-
                                      HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
00a0c906bed8}[deviceinstance]
  Queries value:
HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[service]
HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[classguid]
   Queries value
                                      HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
08002be10318}[lowerfilters]
  Oueries value
HKLM\system\currentcontrolset\enum\umb\1&841921d&0&printerbusenumerator[lowerfilters]
  Oueries value:
                                      HKLM\svstem\currentcontrolset\services\umbus\enum[count]
                                      HKLM\system\currentcontrolset\services\umbus\enum[0]
HKLM\software\microsoft\cryptography\oid\encodingtype
   Queries value:
  Queries value:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7[name]
                                      HKLM\system\currentcontrolset\services\umbus\enum[1]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\enum\umb\umb\18841921d&0&printerbusenumerator[upperfilters]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
Queries value: INCLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7[name]
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
   Oueries value:
                                      HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
   Queries value:
  Oueries value:
HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[spoolsv]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Oueries value:
                                      HKLM\software\microsoft\windows\currentversion[devicepath]
   Queries value
                                      HKLM\system\currentcontrolset\control\wmi\security[c9bf4a9e-d547-4d11-
8242-e03a18b5be011
                                      Queries value:
   Queries value:
                                      HKLM\system\currentcontrolset\control\print[threadnotifyidlelife]
   Oueries value:
   Queries value:
                                       HKLM\system\currentcontrolset\control\print[threadnotifysleep]
  Oueries value:
                                      HKLM\system\currentcontrolset\control\print[maxrpcsize]
                                      HKLM\system\currentcontrolset\control\print[maxrpccalls]
HKLM\software\microsoft\sqmclient\windows\disabledprocesses[71e8376c]
   Queries value:
   Queries value:
                                      Oueries value
   Queries value:
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableipsourcerouting]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[arpretrycount]
                                      HKLM\system\currentcontrolset\services\tcpip\parameters[igmplevel]
HKLM\system\currentcontrolset\services\tcpip\parameters[igmpversion]
   Oueries value
   Queries value
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
  Queries value:
\label{local_HKLM} HKLM \noindent \noindent\
HKLM\system\currentcontrolset\services\tcpip\parameters[disabletaskoffload]
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[enablebcastarpreply]
    Oueries 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
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablemediasenseeventlog]
   Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtudiscovery]
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpuserfc1122urgentpointer]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdataretransmissions]
   Oueries value:
                                                               HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcptimedwaitdelay]
   Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpfinwait2delay]
   Oueries value:
HKLM \label{eq:hkkm} HKLM \label{eq:hkkm} HKLM \label{eq:hkkm} White \label{eq:hkkm} HKLM \label{eq:hkkm} White \label{eq:hkkm} Wh
                                                               HKLM\system\currentcontrolset\services\tcpip\parameters[tcp1323opts]
                                                               HKLM\system\currentcontrolset\services\tcpip\parameters[enabletcpa]
HKLM\system\currentcontrolset\services\tcpip\parameters[enabledca]
    Oueries value:
    Queries value:
   Oueries 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\tcpip\parameters[enableconnectionratelimiting]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
   Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKL
    Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} and $$current control set \end{tabular} $$ ipauto configuration enabled $$\end{tabular} $$
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationsubnet]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationmask]
   Queries value:
Queries value:
                                                               HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter] HKLM\system\currentcontrolset\services\tcpip\parameters[arpuseethersnap]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [overrided efault address selection]
                                                               HKLM\svstem\currentcontrolset\services\tcpip\parameters[maxuserport]
   Oueries value:
    Oueries value:
.
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[ipaddress]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[subnetmask]
Queries value:
c19ce8a73253}[ipautoconfigurationaddress]
   Oueries value:
HKLMNsystem \current control set \services \tcpip \parameters \tinter faces \ \{128919e8-8a5e-41d1-ac17-c19c8a73253\} \ [ipautoconfiguration enabled]
   Oueries value
c19ce8a73253}[performrouterdiscoverv]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[defaultgateway]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[defaultgatewaymetric]
   Queries value:
c19ce8a73253}[solicitationaddressbcast]
   Oueries value:
c19ce8a73253}[usezerobroadcast]
   Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[typeofinterface]
    Queries value
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[mtu]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[interfacemetric]
   Queries value
c19ce8a73253}[tcpackfrequency]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[tcpdelackticks]
   Queries value:
Queries value:
                                                               HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
HKLM \setminus system \setminus current control set \setminus services \setminus language and varieties (rpc cachetime out)
   Queries value:
                                                               HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a544a85b]
HKLM\software\microsoft\com3[finalizeractivitybypass]
    Oueries value:
                                                               HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid[]
HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
    Oueries value:
    Queries value:
   Oueries value:
                                                                HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid[]
    Queries value:
                                                                HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}[]
                                                                {\tt HKLM \ } {\tt System \ } {\tt current control set \ } {\tt vss \ } {\tt settings [idletime out]}
   Oueries value:
    Queries value:
                                                                HKLM\system\setup[upgradeinprogress]
    Queries value:
HKLM\system\currentcontrolset\services\vss\settings[activewriterstatetimeout]

Queries value: HKLM\system\currentcontrolset\services\vss\diag[]

Queries value: HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
                                                               HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid[]
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}[]
    Queries value:
    Queries value:
                                                            HKCR\clsid\{4e14fba2-2e22-11d1-9964-
ver32[inprocserver32]
   Oueries value
00c04fbbb345}\inprocser
                                                               HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[]
   Oueries value:
Queries value: HKCR\clsid\4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocserver32[threadingmodel]
                                                               HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
   Oueries value
    Queries value:
                                                                HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                                                Oueries value:
                                                               HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[]
HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
    Queries value:
   Queries value:
 00c04fb926af\} inprocserver32[inprocserver32] \\ Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af\} inprocserver32[] \\
   Oueries value:
                                                               HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[threadingmodel]
```

```
HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
  Oueries value:
                                    HKCR\interface\{00000100-0000-0000-0000-00000000046}\proxystubclsid32[] HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbb345}\proxystubclsid32[]
  Oueries value:
  Queries value:
  Oueries value:
                                    HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid[]
                                    HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
  Queries value
  Oueries value
                                    HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
  Oueries value
                                    HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocserver32[threadingmodel]
 Oueries value:
                                   HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
                                   HKCR\interface\{0000000c-0000-0000-0000-00000000046}\proxystubclsid32[]
HKLM\software\microsoft\windows nt\currentversion\svchost[wersvcgroup]
  Queries value:
  Queries value:
  Oueries value
                                    HKLM\system\currentcontrolset\services\wersvc\parameters[servicedll]
  Queries value:
HKLM\svstem\currentcontrolset\services\wersvc\parameters[servicemanifest]
                                   HKLM\system\currentcontrolset\services\wersvc\parameters[servicemain]
HKLM\system\currentcontrolset\control\wmi\security[6851adeb-79da-4250-
  Queries value:
  Queries value:
a440-f1f52d28711d1
  Queries value:
                                    HKLM\software\microsoft\windows\windows error reporting[servicetimeout]
  Oueries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set vices \end{tabular} value \current control set \end{tabular} set vices \end{tabular} and \current control set \end{tabular} set vices \end{tabular} when \end{tabular} set vices \end{tabular} when \end{tabular} set vices \end{tabular} set vices \end{tabular} when \end{tabular} set vices \end{tabular} set vices \end{tabular} set vices \end{tabular} when \end{tabular} set vices \end{tabular} set vices
                                    HKLM\software\microsoft\windows nt\currentversion\svchost[imgsvc]
  Queries value:
  Oueries value
                                    {\tt HKLM \ } system \verb| current control set \verb| services \verb| stisvc \verb| parameters [serviced l1]|
  Queries value:
HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest]
  Queries value:
                                    HKLM\system\currentcontrolset\services\stisvc\parameters[servicemain]
  Queries value:
Oueries value:
\label{local_hammon} \begin{tabular}{lllll} HKLM\system\currentcontrolset\control\stillimage\trace[defaulttraceflags] \\ \end{tabular}
  Queries value:
                                   HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracemask]
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracelevel]
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaultmaxtracearraysize]
  Queries value:
Queries value:
  Oueries value:
Oueries value:
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracelevel]
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dllfmaxtracearraysizel
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[enableobjecttracking]
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[heapoptions]
  Oueries value:
                                   HKLM\software\microsoft\rpc\securityservice[10]
  Queries value:
                                   \label{local-hkcR} HKCR\appid\alfaler26-8cfl-11d1-bf92-0060081ed811\ [authenticationlevel] \\ HKCR\appid\alfaler26-8cfl-11d1-bf92-0060081ed811\ [accesspermission] \\
  Queries value:
  Oueries value:
                                    HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811\}\progid[]\\
  Queries value:
                                    HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[]
                                   HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes [34dba8a7] \\ HKCR \setminus clsid \setminus \{b6c292bc-7c88-41ee-8b54-8ec92617e599\}[] \\ HKLM \setminus system \setminus current control set \setminus control \setminus stillimage [deviceid]
  Oueries value:
  Queries value:
  Queries value:
  Oueries value:
Oueries value:
                                   HKLM\system\currentcontrolset\control\stillimage\events\connected[guid]
  Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\connected\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[name]
\label{lem:hklmsystem} HKLM\system\currentcontrolset\control\stillimage\events\connected\{38f8a702-36bb-4a68-80e6-d4966b9b718\}[desc]}
 Queries value
\label{limage-events-connected-438f8a702-36bb-4a68-80e6-d4966b9bb718} [icon] \\
  Oueries value:
HKLMNsystem \current control still image \events \connected \ \{38f8a702-36bb-4a68-80e6-d4966b9b718\} \ [cmdline]
  Oueries value
Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[guid]
  Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\emailimage[guid]
  Oueries value:
.
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[name]
759eb35cdf9a}[desc1
  Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
  Queries value:
Queries value.

HKLMIsystem\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
  Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\faximage[defaulthandler]

Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage[guid]
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[name]
Queries value:

HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc1
  Queries value:
HKLM\system\currentcontrol\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
  Queries value:
Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\printimage[defaulthandler]
                                   HKLM\system\currentcontrolset\control\stillimage\events\printimage[guid]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[name1
  Queries value
```

```
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc]
   Queries value:
\label{limage} HKLM\system\currentcontrolset\control\stillimage\events\printimage\d13e3f25-1688-45a0-9743-759eb35cdf9a\grayer{licon}
   Oueries value:
HKLMNsystem\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a\}[cmdline]}
   Oueries value
HKLM \setminus system \setminus current controls et \setminus control \setminus stillimage \setminus events \setminus scanbutton [defaulth and ler]
  Oueries value:
                                             HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[guid]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[name]
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[desc]
   Queries value:
\label{limage} HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-d4966b9b718\}[icon]}
   Oueries value:
Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}[name]
   Queries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}[desc]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}[icon]
   Queries value:
\label{limage} HKLM \noindent \noi
   Oueries value
759eb35cdf9a}[name]
759eb35cdf9a}[desc]
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
Queries value:
759eb35cdf9a}[cmdline]
   Oueries value:
HKLMNsystem \current control set \control \stillimage \events \scan button \eabbd 70d-a 25f-4e 90-96a 4-7105 fd 3b 53b 1\} [name] \\
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}[desc1
   Queries value:
HKLM \ system \ current control \ stillimage \ events \ scanbutton \ \{eabbd70d-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a4-a25f-4e90-96a6-a25f-4e90-96a6-a25f-4e90-96a6-a25f-4e90-96a6-a25f-4e90-96a6-a25f-4e90-96a6-a25f-4e90-96a6-
7105fd3b53b1}[icon]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}[cmdline]
  Queries value
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[guid]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\serversettings[shutdownifunuseddelay]
                                             HKLM\system\currentcontrolset\services\nativewifip[imagepath]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\nativewifip[objectname]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\nativewifip[type]
   Queries value:
                                             HKLM\system\currentcontrolset\services\nativewifip\enum[count]
HKLM\system\currentcontrolset\services\nativewifip[displayname]
   Queries value:
   Oueries value:
                                              HKLM \verb|\system| current controlset \verb|\enum| root \verb|\legacy_native wifip \verb|\system| service]
   Queries value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[classguid]
Queries value: HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-0000f8753ed1\[lowerfilters]
   Oueries valu
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[lowerfilters]
   Oueries value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[upperfilters]
                                             HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-
  Queries value:
0000f8753ed1}[upperfilters]
                                              HKLM\system\currentcontrolset\services\nativewifip[pnpflags]
   Queries value:
   Oueries value:
                                             HKLM\system\currentcontrolset\control\wmi\security[d905ac1c-65e7-4242-
99ea-fe66a8355df8]
                                             HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
  Queries value:
Queries value: nkm\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterruntype]

Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterclass]
Queries value: 
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
   Oueries value:
                                             HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
                                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage[upperbind]
  Queries value:
Queries value:
                                             HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage[upperbind]

Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
   Queries value:
   Oueries value:
HKLMNsystem\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Oueries value:
                                              HKLM\svstem\currentcontrolset\services\ndisuiofobjectnamel
                                             HKLM\system\currentcontrolset\services\ndisuio[type]
HKLM\system\currentcontrolset\services\ndisuio[type]
   Queries value:
   Queries value
08002be10318}\0006\linkage[upperbind]

Queries value: HKLM\system\currentcontrolset\services\ndisuio\enum[count]
   Oueries value:
                                              HKLM\svstem\currentcontrolset\services\ndisuio[displayname]
   Queries value:
                                              HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
                                              HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[classguid]
   Queries value:
   Oueries value
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[lowerfilters]
   Oueries value:
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[upperfilters]
```

```
Oueries value:
                                   HKLM\svstem\currentcontrolset\services\ndisuio[pnpflags]
  Oueries value
                                   HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-
aded-5304bf8f636d]
  Oueries value
                                   HKLM\svstem\currentcontrolset\control\wmi\securitv[b3eee223-d0a9-40cd-
adfc-50f1888138ab]
  Oueries value:
                                   HKLM\system\currentcontrolset\enum\root\ms sstpminiport\0000[driver]
  Queries value
                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[upperbind]
  Oueries value
                                   HKLM\svstem\currentcontrolset\enum\root\ms pptpminiport\0000[driver]
  Queries value
                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage[upperbind]
  Queries value
                                   HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
08002be10318}\0004\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000[driver]
  Oueries value
                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage[upperbind]
                                   HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
  Queries value:
Oueries value:
                                   HKLM\svstem\currentcontrolset\enum\root\*teredo\0000[driver
Queries value: HKLM\system\08002be10318\\0011\linkage[upperbind]
                                   HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                   HKLM\system\currentcontrolset\enum\root\*isatap\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Oueries value
  Queries value
08002be10318}\0009\linkage[upperbind]
  Queries value
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
  Oueries value:
                                   HKLM \verb|\system| current controlset \verb|\control| \verb|\wmi| autologger \verb|\circular| kernel \\
context logger[start]
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Oueries value
context logger[flushthreshold]
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Queries value
context logger[buffersize]
Queries value:
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[minimumbuffers]
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[flushtimer]
  Queries value
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maximumbuffers]
  Oueries value
                                   HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filename]
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Oueries value
context logger[enablekernelflags]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[stackwalkingfilter]
  Queries value
                                   {\tt HKLM \control \c
context logger[clocktype]
  Queries value
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maxfilesize]
  Oueries value
                                   HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[logfilemode]
                                   HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
  Oueries value
context logger[disablerealtimepersistence]

Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[guid]
  Queries value:
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filecounter]
  Queries value
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filemax]
  Oueries value
                                   HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[pooltagfilter]
  Oueries value
                                   HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-
af71-3e63d056f1741
  Sets/Creates value
                                   HKLM\system\currentcontrolset\enum\root\legacy_nativewifip[nextinstance]
  Sets/Creates value
Sets/Creates value:
                                   HKLM\system\currentcontrolset\enum\root\legacv nativewifip\0000[service]
  Sets/Creates value
                                   HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[legacy]
  Sets/Creates value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[configflags]
Sets/Creates value: HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[class]
  Sets/Creates value
HKLM \verb|\system| current controlset \verb|\enum| root \verb|\legacy_native wifip \verb|\system| class guid]
  Sets/Creates value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[devicedesc]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip\enum[0]
  Sets/Creates value
                                   HKLM\svstem\currentcontrolset\services\nativewifip\enum[count]
                                    HKLM\system\currentcontrolset\services\nativewifip\enum[nextinstance]
  Sets/Creates value
  Sets/Creates value
\label{local-hklm} HKLM\system\currentcontrolset\enum\root\legacy\_native\wifip\0000\control[activeservice] \\ Sets/Creates\ value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
  Sets/Creates value
                                   HKLM\system\currentcontrolset\services\nativewifip[ndismajorversion]
HKLM\system\currentcontrolset\services\nativewifip[ndisminorversion]
  Sets/Creates value
  Sets/Creates value
                                    HKLM\system\currentcontrolset\enum\root\legacy_ndisuio[nextinstance]
   Sets/Creates value
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000\control[*newlycreated*]
  Sets/Creates value:
                                    HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
                                   HKLM\system\currentcontrolset\enum\root\legacv ndisuio\0000[legacv]
  Sets/Creates value
                                   HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[configflags] HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[class]
  Sets/Creates value
  Sets/Creates value:
                                   \label{thm:loss} HKLM \system \current control set \enum \noot \legacy_n disuio \noon [class guid] \\ HKLM \system \current control set \enum \noot \legacy_n disuio \noon [deviced esc] \\
  Sets/Creates value
   Sets/Creates value
  Sets/Creates value
                                   HKLM\svstem\currentcontrolset\services\ndisuio\enum[0]
  Sets/Creates value
                                    HKLM\system\currentcontrolset\services\ndisuio\enum[count]
  Sets/Creates value
                                    HKLM\system\currentcontrolset\services\ndisuio\enum[nextinstance]
  Sets/Creates value
HKLM\system\currentcont
                                  olset\enum\root\legacy_ndisuio\0000\control[activeservice]
  Sets/Creates value:
                                   HKLM\system\currentcontrolset\services\ndisuio[ndismajorversion]
                                   HKLM\system\currentcontrolset\services\ndisuio[ndisminorversion]
HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
  Sets/Creates value
  Value changes:
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
32c86e1ba19f}\#\control[linked]
  Value changes:
                                   HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e
32c86e1ba19f}\control[referencecount]
  Value changes:
                                   HKLM\system\currentcontrolset\services\umbus\enum[count]
   Value changes:
                                    HKLM\system\currentcontrolset\services\umbus\enum[nextinstance]
  Value changes:
                                   HKLM\system\currentcontrolset\services\nativewifip\enum[count]
  Value changes:
                                    HKLM\system\currentcontrolset\services\nativewifip\enum[nextinstance]
                                   HKLM\system\currentcontrolset\services\ndisuio\enum[count]
  Value changes:
  Value changes:
                                   HKLM\system\currentcontrolset\services\ndisuio\enum[nextinstance]
  Value changes:
                                   HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[status]
```