# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Task ID: Risk Level:

Date Processed: 2016-04-08 16:37:32 (UTC)

61.2 seconds IntelliVM Processing Time

Virtual Environment:

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

Sample ID basic Type: Owner: admir

ToggleService32.exe Date Added: 2016-04-08 16:37:32 (UTC)

File Type: PE32:win32 File Size: 10254 bytes

MD5 1439e0552127dda0c66b7be1eadb723d

SHA256: 89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a

Description:

### Pattern Matching Results

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

3 Long sleep detected 6 Writes to system32 folder

6 Modifies registry autorun entries 2 PE: Nonstandard section

5 Installs service

Program causes a crash [Info]
 Terminates process under Windows subfolder

#### Static Events

Anomaly PE: Contains a virtual section

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] C:\Windows\System32\msdtc.exe [C:\Windows\System32\msdtc.exe]
C:\Windows\system32\UI0Detect.exe [C:\Windows\system32\UI0Detect.exe] Creates process: Creates process C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe -

Creates process: LocalServicePeerNet]

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

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

imgsvc]

Loads service:

ALG [C:\Windows\System32\alg.exe]
AppMgmt [C:\Windows\system32\svchost.exe -k netsvcs] Loads service Appmgmit [C.:Windows\system32\svchost.exe -k netsvcs]
BITS [C:\Windows\System32\svchost.exe -k netsvcs]
Browser [C:\Windows\System32\svchost.exe -k netsvcs]
TrkWks [C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted]
MSDTC [C:\Windows\System32\svchost.exe -k NetworkService]
DNSCache [C:\Windows\System32\svchost.exe -k NetworkService] Loads service: Loads service:

Loads service:

Loads service:

Loads service: Loads service: Loads service: EAPHost [C:\Windows\System32\svchost.exe -k netsvcs]
UIODetect [C:\Windows\system32\UIODetect.exe] SharedAccess [C:\Windows\System32\sychost.exe -k netsvcs]
PNRPSvc [C:\Windows\System32\sychost.exe -k LocalServicePeerNet]
Spooler [C:\Windows\System32\spoolsv.exe]
PNRPSvc [C:\Windows\System32\spoolsv.exe] Loads service:

Loads service: Loads service Loads service: Loads service: 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:

LocalSystemNetworkRestricted]

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

LocalServiceNetworkRestricted1

VSS [C:\Windows\system32\vssvc.exe]
AudioSrv [C:\Windows\System32\svchost.exe -k Loads service:

LocalServiceNetworkRestricted]
Loads service: WERSv

WERSvc [C:\Windows\System32\svchost.exe -k WerSvcGroup] Loads service: MpsSvc [C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork]
STISvc [C:\Windows\system32\svchost.exe -k imgsvc]

Loads service: W32Time [C:\Windows\system32\svchost.exe -k LocalService] Loads service: Loads service: Loads service: WUAUServ [C:\Windows\system32\svchost.exe -k netsvcs]
WLANSvc [C:\Windows\system32\svchost.exe -k

LocalSystemNetworkRestricted]
Terminates process: C:\W

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

Creates remote thread

### Named Object Events

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

Creates mutex \BaseNamedObjects\{6979DB2A-DEAA-4E60-B4A4-4051C583B722}\_S-1-5-19 \BaseNamedObjects\WIATRACE\_MUTEX

Creates mutex \BaseNamedObjects\ConsoleEvent-0x00000320
\BaseNamedObjects\SvcctrlStartEvent\_A3752DX Creates event: Creates event Creates event \KernelObjects\MaximumCommitCondition Creates event \Security\LSA\_AUTHENTICATION\_INITIALIZED 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

```
Creates
                                      C:\ProgramData\Microsoft
                                      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\fc45f6fbb5bdaf9f6513a05c5101ab87_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:
                                      C:\Windows\Prefetch\TOGGLESERVICE32_EXE-2248A864_nd
  Onens:
                                      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:
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\Svstem32\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:
  Opens:
   Opens
  Opens:
                                      C:\Windows\Fonts
   Opens:
                                      C:\Windows\Globalization
C:\Windows\Globalization\Sorting
   Opens:
                                      C:\Windows\System32\en-US
C:\Windows\winsxs\x86_microsoft.windows.c.
   Opens:
controls.resources 6595b64144ccf1df 6.0.7600.16385 en-us 581cd2bf5825dde9
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:
                                      C:\Windows\System32\ntdll.dll
C:\Windows\System32\kernel32.dll
  Opens:
                                      C:\Windows\System32\apisetschema.dll
                                      C:\Windows\System32\KernelBase.dll
C:\Windows\System32\locale.nls
  Opens:
                                      C:\Windows\System32\UI0Detect.exe
C:\Windows\System32\advapi32.dll
   Opens:
   Opens
  Opens:
                                      C:\Windows\System32\msvcrt.dll
                                      C:\Windows\System32\rpcrt4.dll
C:\Windows\System32\gdi32.dll
   Opens:
  Opens:
   Opens:
                                      C:\Windows\System32\user32.dl1
C:\Windows\System32\lpk.dl1
   Opens:
                                      C:\Windows\System32\usp10.dll
  Opens:
                                      C:\Windows\System32\wtsapi32.dll
C:\Windows\System32\winsta.dll
   Opens:
  Opens:
                                      C:\Windows\System32\shell32.dll
C:\Windows\System32\shlwapi.dll
   Opens:
   Opens:
  Opens:
                                      C:\Windows\System32\msctf.dll
                                      C:\Windows\System32\en-US\ui0detect.exe.mui
C:\Windows\System32\propsys.dll
   Opens:
  Opens:
                                      C:\Windows\System32\ole32.dll
C:\Windows\System32\oleaut32.dll
   Opens:
   Opens:

        Opens:
        C:\Windows\System32\tzres.dl1

        Opens:
        C:\Windows\System32\tzres.dl1

        Opens:
        C:\Windows\System32\en-US\rgosys.dl1.mui

        Opens:
        C:\Windows\System32\en-US\rgosys.dl1.mui

        Opens:
        C:\Windows\winsx\system32\en-US\rgosys.dl0.mui

        c:\Windows\winsx\system32\en-US\rgosys.dl1.mui

        controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comct132.dl1

  Onens
                                      C:\Windows\WindowsShell Manifest
   Opens:
                                       C:\Windows\System32\duser.dll
  Opens:
                                      C:\Windows\Svstem32\uxtheme.dll
                                      C:\Windows\System32\dwmapi.dl1
C:\Windows\System32\en-US\user32.dl1.mui
   Opens:
   Opens:
                                      C:\Windows\System32\xmllite.dll
C:\Windows\System32\en-US\duser.dll.mui
  Opens
   Opens:
  Opens:
                                      C:\Windows\winsxs\x86 microsoft.windows.c.
controls.resources_6595b64144cf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comct132.dll.mui
Opens: C:\Windows\System32\imageres.dll
                                      C:\Windows\System32\en-US\imageres.dll.mui
C:\Windows\Fonts\StaticCache.dat
   Opens:
   Opens:
  Opens:
                                      C:\Windows\Svstem32\clbcatq.dll
```

C:\Windows\System32\WlS0WndH.dll

```
Opens:
                                        C:\Windows\svstem32\UI0Detect.exe.Local\
   Opens:
                                        C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
                                        C:\$Extend
   Opens:
  Opens:
                                        C:\ProgramData
                                        C:\ProgramData\Microsoft
   Opens:
                                        C:\ProgramData\Microsoft\Crypto
  Opens:
                                       C:\ProgramData\Microsoft\Crypto\RSA
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
   Opens:
  Opens:
  Opens
                                        C:\Windows\Microsoft NFT
                                        C:\Windows\ServiceProfiles
   Opens:
  Opens:
                                        C:\Windows\ServiceProfiles\LocalService
                                       C:\Windows\ServiceProfiles\LocalService\AppData
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
   Opens:
  Opens:
  Opens
                                        C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
   Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier
C:\windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c\grouping
  Opens:
                                       C:\Windows\Svstem32\DriverStore
                                        C:\Windows\System32\DriverStore\en-US
                                        C:\Windows\System32\svchost.exe
  Opens:
  Opens:
                                       C:\Windows\System32\DriverStore\en-US\ndiscap.inf_loc
C:\Windows\System32\userenv.dl1
  Opens:
                                        C:\Windows\Svstem32\profapi.dll
                                       C:\Windows\System32\gpapi.dll
C:\Windows\System32\en-US\svchost.exe.mui
  Opens:
  Opens:
Opens:
                                       C:\Windows\System32\pnrpsvc.dl1
C:\Windows\System32\crypt32.dl1
  Opens:
                                        C:\Windows\System32\msasn1.dll
                                       C:\Windows\System32\en-US\crypt32.dll.mui
C:\WINDOWS\MICROSOFT.NET\NGENSERVICE_PRI1_LOCK.DAT
  Opens:
                                       C:\Windows\System32\ncrypt.dll
C:\Windows\System32\p2pcollab.dll
   Opens:
   Opens:
                                       C:\Windows\System32\en-US\p2pcollab.dll.mui
C:\Windows\System32\QAGENTRT.DLL
C:\Windows\System32\DriverStore\en-US\netrast.inf_loc
  Opens:
   Opens:
  Opens:
   Opens:
                                       C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Windows\System32\fveui.dll
   Opens:
  Opens:
                                       C:\Windows\System32\en-US\fveui.dll.mui
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
  Opens:
                                        C:\Windows\System32\ws2_32.dll
                                        C:\Windows\System32\nsi.dll
   Opens:
                                        C:\Windows\System32\wship6.dll
  Opens:
   Opens:
                                       C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
  Opens:
  Opens:
                                        C:\Windows\Svstem32\dhcpcsvc6.dll
                                        C:\Windows\System32\dhcpcsvc.dll
   Opens:
  Opens:
                                        C:\Windows\Svstem32\sqmapi.dll
   Opens:
                                        C:\Windows\System32\ssdpapi.dll
  Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f6af2fef0fc5f4f2bc6f75c1ff7fd887 577c175f-2428-
49fc-a95e-635c93546ef9
                                        C:\Windows\Svstem32\p2psvc.dll
  Opens:
   Opens:
                                       C:\Windows\System32\P2PGraph.dll
C:\Windows\System32\esent.dll
  Opens:
                                       C:\Windows\System32\slc.dll
C:\Windows\System32\psapi.dll
  Opens
   Opens:
  Opens:
                                        C:\Windows\System32\DriverStore\en-US\nettcpip.inf loc
                                        C:\Windows\System32\authz.dll
   Opens:
  Opens:
49fc-a95e-635c93546ef9
  Opens:
                                        C:\Windows\Svstem32\DriverStore\en-US\lltdio.inf loc
C:\PROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\F0D041F93C731ACAA036AC2BD71BC124_577C175F-2428-
49FC-A95E-635C93546EF9
  Opens:
                                        C:\Windows\System32\DriverStore\en-US\netsstpt.inf_loc
  Opens:
                                        C:\Windows\Svstem32\pnrpnsp.dll
                                        C:\Windows\System32\rasadhlp.dll
   Opens:
  Opens:
\label{lem:c:programData} C: \PogramData\\ Microsoft\\ Crypto\\ RSA\\ Machine Keys\\ eb3bc6388b8f46d91ac65574d706a290\_577c175f-2428-49fc-a95e-635c93546ef9
  Opens:
Opens:
{\tt C:Windows} Service Profiles \\ {\tt LocalService} App Data \\ {\tt Roaming} Peer Networking \\ {\tt 8d844364c535c5b5c8ba03cedd538a73.sstates} \\ {\tt Roaming} {\tt Noaming} {\tt Noaming} {\tt Noaming} \\ {\tt Noaming} {\tt Noaming} {\tt Noaming} {\tt Noaming} \\ {\tt Noaming} {\tt Noaming} {\tt Noaming} \\ {\tt Noaming} {\tt Noaming} {\tt Noaming} \\ 
                                        C:\Windows\System32\Wldap32.dll
  Opens:
  Opens:
                                        C:\Windows\Svstem32\schannel.dll
                                        C:\Windows\System32\DriverStore\en-US\netserv.inf_loc
   Opens:
  Opens:
C:\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\ROAMING\PEERNETWORKING\65E9EDA7BCB6088518AEA0DDF13DF80843A6EA25.HOMEGROUPCLASSIFIER\F8D4F95592CE335421D51FADB8712F5C\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\fc45f6fbb5bdaf9f6513a05c5101ab87_577c175f-2428-
49fc-a95e-635c93546ef9
  Opens:
                                        C:\Windows\System32\en-US\QAgentRT.dll.mui
  Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\14ea4bced676baf04ccdfd43a9e1f75f.sst
Opens: C:\Windows\Prefetch\SP00LSV.EXE-D1F6B8B6.pf
  Opens:
                                       C:\Windows\Svstem32\powrprof.dll
   Opens:
                                        C:\Windows\System32\en-US\spoolsv.exe.mui
                                        C:\Windows\Svstem32\en-US\setupapi.dll.mui
  Opens:
                                       C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
C:\Users
   Opens:
  Opens:
                                        C:\Users\Admin
  Opens
   Opens:
                                        C:\Users\Admin\AppData
                                        C:\Users\Admin\AppData\Local
  Opens:
                                       C:\Users\Admin\AppData\Local\Microsoft
C:\Users\Admin\AppData\Local\Microsoft\Windows
   Opens:
   Opens:
                                       Onens:
   Opens
Files\Content.IE5
                                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\KQ5TVCON
                                       C:\Users\Admin\AppData\Roaming
  Opens
   Opens:
                                        C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:
                                       C:\Users\Admin\AppData\Roaming\Microsoft\Windows C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
```

```
Opens:
                               C:\Windows\SoftwareDistribution
  Opens:
                               C:\Windows\SoftwareDistribution\WuRedir
                               C:\Windows\SoftwareDistribution\WuRedir\9482F4B4-E343-43B6-B170-
  Opens
9A65BC822C77
  Opens:
                               C:\Windows\System32\catroot
  Opens:
                               C:\Windows\Svstem32\VSSVC.exe
                               C:\Windows\System32\vssapi.dll
C:\Windows\System32\vsstrace.dll
  Opens:
  Opens:
                               C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll
  Opens
  Opens:
  Opens:
                               C:\Windows\Svstem32\srvcli.dll
                               C:\Windows\System32\wkscli.dll
C:\Windows\System32\samcli.dll
  Opens:
  Opens:
                               C:\Windows\System32\setupapi.dll
C:\Windows\System32\cfgmgr32.dll
  Opens
  Opens:
  Opens:
                               C:\Windows\Svstem32\devobi.dll
                               C:\Windows\System32\virtdisk.dll
C:\Windows\System32\fltLib.dll
  Opens:
  Opens:
                               C:\Windows\System32\en-US\VSSVC.exe.mui
C:\Windows\System32\vss_ps.dll
  Opens:
  Opens:
  Opens:
                               C:\Windows\Svstem32\en-US\vsstrace.dll.mui
                               C:\Windows\System32\samlib.dll
C:\Windows\System32\es.dll
  Opens:
  Opens:
Opens:
                               C:\Windows\System32\catsrvut.dll
C:\Windows\System32\mfcsubs.dll
  Opens:
                               C:\Windows\Svstem32\rasctrs.dll
                               C:\Windows\System32\sxs.dll
C:\Windows\System32\eventcls.dll
  Opens:
  Opens:
Opens:
                               C:\Windows\System32\stdole2.tlb
C:\Windows\System32\msxml3.dll
  Opens:
                               C:\Windows\Svstem32\en-US\KernelBase.dll.mui
                               C:\Windows\System32\msxml3r.dll
C:\Windows\System32\wintrust.dll
  Opens:
  Opens:
                               C:\Windows\System32\sdclt.exe
  Opens
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\KQ5TVCON\LOCALE-SPECIFIC[1].CSS
                               C:\Windows\Fonts\palab.ttf
C:\WINDOWS\SYSTEM32\CATROOT\TMP1E1E.TMP
  Opens:
  Opens
Opens: C:\WINDOWS\SOFTWAREDISTRIBUTION\WUREDIR\9482F4B4-E343-43B6-B170-9A65B622C77\WUREDIR.CAB.BAK
                               C:\WINDOWS\SYSTEM32\CATROOT\TMP26E3.TMP
  Opens:
                               C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
  Opens:
  Opens:
                               C:\Windows\System32\wersvc.dll
                               C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
C:\CONFIG.MSI
  Opens:
  Opens:
                               C:\CONFIG.MSI\41EA3.RBF
C:\CONFIG.MSI\41F56.RBF
  Opens:
  Opens:
                               C:\Windows\System32\wiaservc.dll
C:\Windows\System32\msv1_0.dll
C:\CONFIG.MSI\41F57.RBF
  Opens:
  Opens:
  Opens:
                               C:\Windows\System32\wiatrace.dll
C:\Windows\debug\WIA\wiatrace.log
  Opens:
  Opens:
  Opens
                               C:\Windows\Svstem32\drivers\nwifi.svs
                               C:\Windows\AppPatch\drvmain.sdb
  Opens:
                               C:\Windows\Svstem32\drivers\etc\lmhosts
  Opens:
  Opens:
                               C:\Windows\System32\drivers\ndisuio.sys
C:\Windows\System32\drivers\spsys.sys
  Opens:
  Onens
                               C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-
A289-439d-8115-601632D005A0
                               C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-
 Opens
A289-439d-8115-601632D005A0
                               C:\Windows\System32\drivers\asyncmac.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\fc45f6fbb5bdaf9f6513a05c5101ab87_577c175f-2428-
49fc-a95e-635c93546ef9
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
 Reads from:
Reads from:
                               C:\Windows\System32\output.txt
C:\Windows\Prefetch\UIODETECT.EXE-A794C8BB.pf
  Reads from:
                               C:\Windows\Fonts\StaticCache.dat
                               C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
  Reads from
  Reads from
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
  Reads from:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Reads from: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Reads from: C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
Windows Registry Events
                               HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%11/8
  Creates key:
                               HKLM\svstem\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e 32c86e1ba19f}\control
32c86e1ba19f}\#\control
                               HKLM\system\currentcontrolset\control\deviceclasses
HKCU\software\classes\local settings\muicache\27\52c64b7e
HKCU\software\classes\local settings\muicache
HKLM\system\currentcontrolset\services\umbus\enum
  Creates key:
  Creates key:
  Creates key:
  Creates key:
  Creates key:
                               HKLM\software\classes
Creates key:
08002be10318}\0007
                               Creates key:
08002be10318}\0006
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                               HKLM\system\currentcontrolset\services\vss\diag\registry writer
 Creates key:
                               HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
HKLM\system\currentcontrolset\services\vss\diag\asr writer
  Creates key:
  Creates key
Creates key:
writer
                               \label{localization} \mbox{HKLM} \mbox{\sc system} \mbox{\c copy optimization}
 Creates key
                               HKLM\system\currentcontrolset\control\stillimage\trace
  Creates key:
                               HKLM\system
HKLM\system\currentcontrolset
  Creates key:
  Creates key:
                               HKLM\system\currentcontrolset\control
HKLM\system\currentcontrolset\control\stillimage
  Creates key:
  Creates key
                               HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll
```

```
Creates key:
                                                    HKLM\svstem\currentcontrolset\services\nativewifip\enum
    Creates key
                                                    HKLM\system\currentcontrolset\enum\root\legacy_nativewifip
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
   Creates key:
   Creates key
                                                   \label{thm:loss} HKLM \system \current control set \enum \noot \legacy\_native wifip \0000 \control \noonup \
    Creates key
   Creates key
                                                    HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters
   Creates key
                                                   HKLM\system\currentcontrolset\services\nativewifip
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Creates key:
08002he103183\0005
Creates key:
08002be10318}\0008
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                                    HKLM\system\currentcontrolset\services\ndisuio\enum
    Creates key
   Creates key:
                                                    HKLM\system\currentcontrolset\enum\root\legacy_ndisuio
   Creates key
                                                   \label{thm:loss} HKLM \system \current control set \enum \root \legacy\_n disuio \control \enum \root \legacy\_n disuio \control \enum \root \legacy\_n disuio \control \enum \root \legacy\_n \enum \root \ro
   Creates key
   Creates key
                                                    HKLM\svstem\currentcontrolset\services\ndisuid
Creates key:
08002be10318}\0000
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Creates key:
08002be10318}\0003
                                                    HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Creates key
                                                    HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Creates key:
08002he103183\0002
Creates key:
08002be10318}\0001
                                                    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\control\class\{4d36e972-e325-11ce-bfc1-
   Creates kev:
                                                    HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac
                                                    HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
   Creates key:
00805fc1270e}\asyncmac\control
                                                    HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
   Creates key:
00805fc1270e}\asvncmac\logconf
    Creates key:
                                                    HKLM\system\currentcontrolset\services\asyncmac\en
                                                    HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Creates key
08002be10318}\0010
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
   Creates key:
82e6-71a87abac361}
                                                    82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03
82e6-71a87abac361}
Creates key:
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}\#
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Creates key:
8dcb-00c04fc3358c}
                                                   HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Creates kev:
8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#{e2f8a220-af88-446c-9a55-453e58dd3a33}
   Creates key
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}\control
Creates key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}\#\control
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#
8dcb-00c04fc3358c}\control
   Creates key:
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\#{e2f8a220-af88-446c-9a55-453e58dd3a33}\control
   Deletes value:
                                                   HKLM\svstem\currentcontrolset\services\umbus\enum[1]
                                                    HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
    Deletes value
00805fc1270e}\asyncmac\logconf[basicconfigvector]
Deletes value: HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-00805fc1270e}\asyncmac\logconf[bootconfig]
                                                    HKLM\svstem\currentcontrolset\control\session manager
   Opens kev:
    Opens key:
                                                   HKLM\system\currentcontrolset\control\terminal server
HKLM\system\currentcontrolset\control\safeboot\option
   Opens key:
                                                   HKLM\system\currentcontrolset\control\srp\gp\dll HKLM\software\policies\microsoft\windows\safer\codeidentifiers
    Opens key:
    Opens key:
   Opens kev:
                                                    HKCU\software\policies\microsoft\windows\safer\codeidentifiers
    Opens key:
                                                    HKCU\control panel\desktop\muicached\machinelanguageconfiguration
   Opens key:
                                                   HKLM\software\policies\microsoft\mui\settings
HKCU\software\policies\microsoft\control panel\desktop
    Opens key:
    Opens key:
                                                   HKCU\control panel\desktop\languageconfiguration
HKCU\control panel\desktop
HKCU\control panel\desktop\muicached
   Opens key:
    Opens key:
   Opens key:
   Opens key:
Opens key:
                                                   HKLM\software\microsoft\windows\currentversion\sidebyside
HKLM\system\currentcontrolset\control\nls\sorting\versions
   Opens key:
                                                    HKLM\
    Opens key:
                                                    HKLM\software\microsoft\windows nt\currentversion\diagnostics
   Opens key:
                                                    HKLM\software\microsoft\rpc
   Opens key:
Opens key:
                                                    HKLM\system\currentcontrolset\control\computername\activecomputername
                                                    HKLM\system\setup
                                                    HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                                    HKLM\software\policies\microsoft\sqmclient\windows
    Opens key:
                                                    HKLM\software\microsoft\samclient\windows
   Opens key:
                                                   HKLM\system\currentcontrolset\control\sqmservicelist
HKLM\system\currentcontrolset\control\mui\settings
    Opens key:
    Opens key:
                                                   \label{thm:local_ham} \begin{tabular}{ll} HKLM\system\currentcontrolset\control\error\ message\ instrument \\ HKLM\system\currentcontrolset\control\error\ message\ instrument \\ \end{tabular}
   Opens kev
    Opens key:
   Opens key:
                                                    HKLM\software\microsoft\windows nt\currentversion\gre initialize
                                                   HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility
    Opens key:
    Opens key:
    Opens key
                                                    HKLM\svstem\currentcontrolset\control\cmf\config
    Opens key:
                                                    HKLM\software\microsoft\windows nt\currentversion\windows
   Opens key:
                                                    HKLM\software\microsoft\ole
                                                   HKLM\software\microsoft\ole\tracing
HKLM\software\microsoft\oleaut
    Opens key:
    Opens key:
    Opens key
                                                    HKCII\software\classes\
    Opens key:
                                                    HKLM\software\classes
   Opens kev:
                                                    HKLM\software\microsoft\com3
                                                   HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\treatas
    Opens key:
    Opens key:
    Opens key
                                                    HKCR\clsid\\d6015ec3-fa16-4813-9ca1-da204574f5da\\progid
HKCR\clsid\\d6015ec3-fa16-4813-9ca1-da204574f5da\\inprocserver32
    Opens key:
   Opens key:
                                                    HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler32
                                                    HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler
```

```
Opens key:
                                    HKCR\appid\alg.exe
                                    HKLM\software\microsoft\ole\appcompat
HKLM\system\currentcontrolset\control\lsa
  Opens key
  Opens key:
  Opens kev
                                    {\tt HKLM \coftware \microsoft \cryptography \cdefaults \provider \microsoft \ strong}
cryptographic provide
  Opens key:
                                    HKLM\svstem\currentcontrolset\control\lsa\fipsalgorithmpolicv
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:
                                   HKLM\software\policies\microsoft\cryptography
HKLM\software\microsoft\cryptography
  Opens key:
                                   HKLM\software\microsoft\cryptography\offload
HKCR\interface\{0000134-0000-0000-c000-00000000046}\HKCR\interface\{0000134-0000-0000-c000-00000000046}\proxystubclsid32
  Opens key:
  Opens key:
  Opens key:
  Opens key:
                                   HKLM\software\microsoft\rpc\extensions
HKLM\system\currentcontrolset\services\bfe
  Opens key:
                                   \label{lem:hklmsoftware\microsoft} HKLM\software\microsoft\sqmclient\windows\disabledsessions \hkcR\clsid\f8ade1d3-49df-4b75-9005-ef9508e6a337\}
  Opens key:
  Opens key:
  Opens key:
  Opens key:
                                    HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
                                   HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
  Opens key:
  Opens key:
                                    HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
  Opens key:
  Opens key:
  Opens key:
                                    HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267999}
HKCR\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
  Opens key:
                                    HKLM\software\microsoft\alg\isv
                                   HKLM\software\microsoft\msdtc\tracing
HKLM\software\microsoft\msdtc\tracing\sources
  Opens key:
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\msdtc\tracing\output
HKLM\software\microsoft\msdtc
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc
  Opens key:
                                   HKCR\cid.local
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a
  Opens key:
  Opens key:
                                    \label{local-1} HKCR\cid.local\angle 979c-4ebb-9e3e-a23014be3f1a\description HKCR\cid.local\angle 9619d-4d5f-a782-28d960ea489d
  Opens key:
                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\description
                                    HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5
HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5\description
  Opens key:
  Opens key:
  Opens key:
                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\description
  Opens key:
                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed
                                   HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\description
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid
  Opens key:
  Opens key:
  Opens key:
Opens key:
                                    HKCR\svcid.local
                                    HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464
  Opens key:
                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\host
                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\clsid
HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
  Opens key:
  Opens key:
  Opens key:
Opens key:
                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\protocol
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\endpoint
                                   Opens key:
  Opens key:
  Opens key
782ab52d45ed\customproperties\log\size
Opens key: HKLM\software\microsoft\msdtc\mtxoci
  Opens key
                                    HKLM\software\microsoft\msdtc\security
                                    HKLM\software\microsoft\windows nt\currentversion\asr\restoresession
  Opens key:
  Opens key
                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
782ab52d45ed \verb|\customproperties\verb|\log\verb|\path|
  Opens key:
                                   HKLM\software\microsoft\windows
\label{lem:nt-current} $$ nt'currentversion \tracing\mbox{$\mathbb{N}$ opens key:} $$ HKLM\system\currentcontrolset\control\mbox{$\mathbb{N}$ opens} $$
  Opens key:
                                    HKLM\svstem\currentcontrolset\control\timezoneinformation
  Opens key:
                                   \label{thm:local_hklm} HkLm\software\microsoft\windows nt\currentversion\tracing\msdtc\modules HkLm\software\microsoft\windows
  Opens key:
nt\currentversion\tracing\msdtc\modules\transaction_transitions
                                    HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed
  Opens key:
  Opens kev:
                                    HKLM\software\microsoft\windows nt\currentversion
  Opens key:
                                   HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\svcid
HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464
  Opens key:
  Opens key:
                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\host
                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\clsid
  Opens key:
  Opens key:
                                    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:
                                    HKCU\control panel\international HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:
  Opens key:
  Opens key:
                                    HKLM\svstem\currentcontrolset\control\nls\extendedlocale
  Opens key
                                    HKLM\software\microsoft\rpc\securityservice
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
  Opens key:
                                    HKLM\system\currentcontrolset\control\securityproviders
  Opens key:
  Opens key:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\customproperties
  Opens key:
  Opens key:
  Opens key:
  Opens key:
Opens key:
                                    \label{thm:hkcrcid.local} HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\customproperties\dack{hkLM}\system\currentcontrol\sta^accessproviders
  Opens key:
                                    HKLM\svstem\currentcontrolset\services\ldap
  Opens key:
                                    HKCR\cid.local\1199661d8-979c-4ebb-9e3e-a23014be3f1a\svcid
HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef
  Opens key:
  Opens key:
Opens key:
                                    HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\host
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\clsid
  Opens key:
                                    HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider
  Opens key:
                                   HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\endpoint
  Opens key:
  Opens key:
Opens key:
                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\svcid
HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
  Opens kev
                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\host
  Opens key:
                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\clsid
HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider
  Opens key:
                                    HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\protocol
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\endpoint
  Opens key:
  Opens key:
  Opens key
                                    HKIM\software\microsoft\windows\windows error reporting\wmn
                                   HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
  Opens key:
  Opens key:
                                    HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
  Opens key:
  Opens key:
  Opens key
                                    HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
  Opens key:
                                    HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
  Opens key:
                                    HKLM\svstem\currentcontrolset\control\computernam
```

Opens key: HKU\.default\control panel\desktop\muicached\machinelanguageconfiguration Opens key: Opens key:

HKU\.default\software\policies\microsoft\control panel\desktop
HKU\.default\control panel\desktop\languageconfiguration

Opens key: HKU\.default\control panel\desktop

HKU\.default\control panel\desktop\muicached

```
Opens kev:
                                      HKU\.default\control panel\international
                                      HKLM\software\microsoft\ctf\compatibility\ui0detect.exe
HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
   Opens key:
  Opens key
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                      HKLM\software\microsoft\ctf\
   Opens key:
  Opens key:
                                      HKLM\software\microsoft\ctf\knownclasses
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:
                                      HKI M\software\microsoft\directui
   Opens key:
                                      HKLM\system\currentcontrolset\control\nls\locale
  Opens key:
                                      HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens key:
                                      HKLM\system\currentcontrolset\control\nls\language groups
HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
   Opens key:
Opens key: HKLM\software\micros nt\currentversion\languagepack\datastore_v1.0
                                      HKI M\software\microsoft\windows
  Opens key:
                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
Openskey: HKLM\software\microsoft\windows nt\currentversion\svchost
  Opens key:
                                      HKLM\software\microsoft\windows
nt\currentversion\svchost\localservicepeernet
                                      HKLM\system\currentcontrolset\services
  Opens key:
   Opens key:
                                      HKLM\system\currentcontrolset\services\p2pimsvc
HKLM\system\currentcontrolset\services\p2pimsvc\parameters
   Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens kev:
   Opens key:
                                      HKLM\software\policies\microsoft\windows\system
HKLM\software\policies\microsoft\peernet
  Opens key:
  Opens key:
Opens key:
                                      HKLM\system\currentcontrolset\services\pnrpsvc
HKLM\system\currentcontrolset\services\pnrpsvc\parameters
  Opens kev:
                                      HKLM\system\currentcontrolset\services\winsock2\parameters
                                      HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
   Opens key:
HKLM\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e4\u00e
HKLM\svstem\currentcontrolset\services\winsock2\parameters\appid catalog\2c69d9f1
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: 
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000003
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000005
  Opens kev:
Opens key:
Opens key: 
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000012
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000013
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000018
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key: 
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\0000000000003
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:
  Opens key:
                                      HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
   Opens key:
                                      HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:
                                      HKLM\system\currentcontrolset\services\winsock\setup
Opens~key: \\ HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17-41d1-ac17
c19ce8a73253}
Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a732533
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKL\dot{M} \rangle system \setminus current control set \ services \ tcpip6 \cap arameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\}
   Opens key
```

```
1709a0196aed3
    Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
    Opens key:
                                                        \label{lem:hklm} \verb+KKLM \system \current control set \services \tcpip \linkage
   Opens key:
                                                        HKLM\software\microsoft\samclient
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp HKLM\software\policies\microsoft\peernet\pnrp\ipv6-linklocal
   Opens key:
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal
   Opens key
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
   Opens kev:
a03a-e3ef65729f3d}\propertybag
   Opens key:
                                                        HKCII\software\microsoft\windows\currentversion\explorer
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0
   Opens key:
                                                        HKU\
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Opens key:
Opens key:
                                                        HKIM\software\microsoft\windows nt\currentversion\nrofilelist
                                                        HKLM\system\currentcontrolset\control\session manager\environment
   Opens key:
                                                        HKLM\software\microsoft\windows\currentversion
    Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
                                                        HKCU\environment
   Opens key:
   Opens key:
Opens key:
                                                       HKCU\volatile environment
HKCU\volatile environment\0
   Opens kev:
                                                        HKLM\software\policies\microsoft\windows\explorer
                                                        HKCU\software\policies\microsoft\windows\explore
     Opens key:
    Opens key:
HKLMNs of tware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions|| \{5e6c858f-0e22-4760-9afe-ea3317b67173\}
9afe-ea3317b67173}\propertybag
   Opens key:
Opens key:
                                                        HKLM\system\currentcontrolset\services\crypt32
                                                        HKLM\software\microsoft\cryptography\oid
   Opens key:
                                                        \label{localization} HKLM \software \mbox{\sc microsoft} \cryptography \sc oid \encoding type 0
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
    Opens key:
0\certdllopenstoreprov
Opens key: HI

O\certdllopenstoreprov\#16
                                                        {\tt HKLM \ } software \verb|\ microsoft \ \\ cryptography \verb|\ oid \ \\ encoding type \\ encoding typ
   Opens key
                                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
                                                        HKLM\software\microsoft\crvptographv\oid\encodingtvpe 1
   Opens kev:
Opens key:
1\certdllopenstoreprov
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
   Opens key
                                                       HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdlldecodeobjectex
                                                       HKLM\software\microsoft\crvptography\oid\encodingtype
   Opens key
1\cryptdlldecodeobjectex
                                                       HKLM\software\microsoft\cryptography\oid\encodingtype
   Opens key:
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
                                                       {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
 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
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\software\microsoft\w:
                                                       HKLM\software\microsoft\windows nt\currentversion\msasn1
HKLM\software\microsoft\cryptography\defaults\provider types\type 012
   Opens key:
Opens key: HKLM\s
schannel cryptographic provider
                                                        HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{$\mbox{$\mbox{$w$are}$} \mbox{$\mbox{$w$are}$} \mbox{$\mbox{$\mbox{$w$are}$} \mbox{$\mbox{$\mbox{$w$are}$}$} \mbox{$\mbox{$\mbox{$\mbox{$w$are}$}$} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$
Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82 - fdc1 - 4dc3 - fdc1 - fd
a9dd-070d1d495d97}\propertybag
    Opens key:
                                                        {\tt HKLM} \verb|\software\microsoft\cryptography\deshashsessionkeybackward
                                                        HKLM\system\currentcontrolset\control\deviceclasses
   Opens key:
Opens key:
843e-32c86e1ba19f}
                                                        HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
   Opens kev:
                                                        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}\#
Opens key:
b082-00a0c91efb8b}
                                                        HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
Opens key:
b082-00a0c91efb8b}\##?
                                                        #pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-
00a0c91efb8b}
                                                       HKLM\svstem\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
   Opens key:
b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&6373acf&0&400008#{2accfe60-
c130-11d2-b082-00a0c91efb8b}
   Opens kev:
                                                       HKLM\svstem\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
                                                       HKLM\svstem\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
   Opens kev:
b082-00a0c91efb8b}\##?#pciide#idechannel#4&Zab44545&0&0#{Zaccfe60-c130-11d2-b082-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&1#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcortrollset\control\deviceclasses\\2acfe60-c130-11d2-b082-00a0c91efb8b\\#?#pciide#idechannel#482d9c6e018080#\{2accfe60-c130-11d2-b082-00a0c91efb8b}\\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#482f42c7138080#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#482f42c7138081#{2accfe60-c130-11d2-b082-00a0c91efb8b}
   Opens key:
                                                       HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
84ae-d30803bae505}
                                                       HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
   Opens key:
84ae-d30803hae505}}\##2#root#ydryroot#0000#{2e34d650-5819-42ca-84ae-d30803hae505}}
Opens key:
bc8c-00a0c91405dd}
                                                       HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
                                                        HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
```

Opens key:

```
bc8c-00a0c91405dd}\##?#acpi#pnp0f03#4&1d401fb5&0#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co102#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-
00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-1bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co102#6&1e20eb37&0&0001#{378de44c-56ef-11d1-bc8c
                                                             00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-1 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}
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
    Onens key
bc8c-00a0c91405dd}\##?#root#rdp_mou#0000#{378de44c-56ef-11d1-bc8c-00a0c91405dd}
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
   Opens key:
8a92-1e6861e6af27}
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
   Opens key:
8a92-1e6861e6af27\} \\ \text{\#?\#pci\#ven\_8086\&dev\_27c8\&subsys\_01e61028\&rev\_01\#3\&2411e6fe\&0\&e8\#\{3abf6f2d-1e6861e6af27\}\}} \\ \text{\#?\#pci\#ven\_8086\&dev\_27c8\&subsys\_01e61028\&rev\_01\#3\&2411e6fe\&0\&e8\#\{3abf6f2d-1e6861e6af26\}\}} \\ \text{\#?\#pci\#ven\_8086\&eaf264} \\ \text{\#pci\#ven\_8086\&eaf264} \\ \text{\#pci\#ven\_8086$} \\ \text{\#pci#ven\_8086$} \\ \text{\#pci#
71c4-462a-8a92-1e6861e6af27}
    Opens kev:
                                                          HKLM\svstem\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-71c4-46
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}
Opens key: HKLM\system\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}
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
    Opens key:
8a92-1e6861e6af27\} \\ \text{\#?\#pci\#ven\_8086\&dev\_27ca\&subsys\_01e61028\&rev\_01\#3\&2411e6fe\&0\&ea\#\{3abf6f2d-1e6861e6af27\}} \\ \text{\#?\#pci\#ven\_8086\&dev\_27ca\&subsys\_01e61028\&rev\_01\#3\&2411e6fe\&0\&ea\#\{3abf6f2d-1e6861e6af26\}} \\ \text{\#?\#pci\#ven\_8086\&eaf264} \\ \text{\#?\#pci\#ven\_8086$} \\ \text{\#pci\#ven\_8086$} \\ \text{\#pci\#ven\_8086$} \\ \text{\#pci\#ven\_8086$} \\ \text{\#pcip\#ven\_8086$} \\ \text{\#pci\#ven\_8086$} \\ \text{\#pcip\#ven\_8086$} \\ \text{\#pcip\#ven\_8
 71c4-462a-8a92-1e6861e6af27]
                                                           HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
    Opens key:
8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&1&ea#{3abf6f2d-
71c4-462a-8a92-1e6861e6af27}
    Opens kev:
                                                          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-71c4-462a-8a92-1e6861e6af27\}\wffere.} \\ NHR/M\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27\}\wffere.} \\ NHR/M\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\wffere.} \\ NHR/M\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\wffere.} \\ NHR/M\system\currentcontrol\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\wffere.} \\ NHR/M\system\currentcontrol\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\devi
71c4-462a-8a92-1e6861e6af27}
Opens key:
b732-99a6111edc0b}
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662-
Opens key:
a5d6-28db04c10000}
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-
   Opens kev:
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-
a5d6-28db04c10000}\##?#root#system#0000#{4747b320-62ce-11cf-a5d6-28db04c10000}
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-
   Opens key:
be5e-00a0c9062857}
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{4afa3d53-74abe5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e-00a0c9062857}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74abe5e-00a0c9062857}\\##?#acpi#fixedbutton#2&daba3ff&1#{4afa3d53-74a7-11d0-be5e-00a0c9062857}
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\\##?\acpi\#fixedbutton\#2&daba3ff\&2\#{4afa3d53-74a7-11d0-be5e-00a0c9062857}\\\\ \end{array}
   Onens key
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e5b2-T1b1-186b-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{4d1e55b2-f16f-11cf-88cb-
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
001111000030}
    Onens key
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&0000#{4dd1e55b2-f16f-11cf-88cb-
001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&1c83c2e&0&0001#{4d1e55b2-f16f-11cf-88cb-
001111000030}
    Opens key:
                                                              HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}\##?#hid#vid 14dd&pid 1005&col02#6&1e20eb37&0&0001#{4d1e55b2-f16f-11cf-88cb
001111000030}
Opens \ key: \\ HKLM\system\currentcontrolset\control\deviceclasses \ \{4d1e55b2-f16f-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-001111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-00111000030\}\ k#?\#hid\#vid\_14dd&pid\_1005&col03\#6&1c83c2e&0&0002\#\{4d1e55b2-f16f-11cf-88cb-00111000030\}\ k#
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
001111000030}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11
88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col03#6&1e20eb37&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
Opens key:
94f2-00a0c91efb8b}
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
Opens key:
94f2-00a0c91efb8b}\##?
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
                                                                                                                       _4.6.2.6_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-
#ide#diskseagate
94f2-00a0c91efb8b}
Opens key:
94f2-00a0c91efb8b}\##?
                                                             HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
 #ide#diskseagate_
                                                                                                                       _5.7.4.5_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}
Opens key:
94f2-00a0c91efb8b}\##?
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
#ide#diskvbox harddisk
                                                                                                                                          #5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
   Opens key:
94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&17b13437&0&000000#{53f56307-b6bf
 11d0-94f2-00a0c91efb8b}
    Opens key:
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&3af2ddc5&0&00000#{53f56307-b6bf-
11d0-94f2-00a0c91efb8b}
Opens key:
94f2-00a0c91efb8b}
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
   Opens kev:
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
                                          ___1.05___#5&23a61b21&0&0.0.0#5(53f56308-b6bf-11d0-94f2-00a0c91efb8b)

HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
t10n
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                                             1.0
                                                                                                 _#5&106af171&0&1.0.0#{53f56308-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\cur 94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
                                                                                                 #5&394c0ad3&0&0.1.0#{53f56308-b6bf-11d0-94f2-
 rom
                                                                            1.0
00a0c91efb8b3
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: 94f2-00a0c91efb8b}
    Opens key:
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st dvd-rom gdr
```

\_1.02\_\_\_\_#5&28836b88&0&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

```
Opens kev:
                                                                     HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-bbbf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
t10n______1.05___#5823a61b218080.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromybox_cd-
                                                                                                            #5&106af171&0&1.0.0#{53f5630d-b6bf-11d0-94f2-
                                                                                       1.0
rom
00a0c91efb8b}
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\cur 94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                                                                         ____#5&394c0ad3&0&0.1.0#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{69d250e0-6c18-11e3-b3bc-
806e6f6e6963}#00000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrol\set\control\
94f2-00a0c91efb8b}\##?#storage#volume#{69d250e0-6c18-11e3-b3bc-
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
806e6f6e6963}#00000000000000#{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}#0000000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
                                                                 HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Opens kev:
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f447-11df-aef6-
806e6f6e6963}#00000075343e000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLMsystem\currentcontrol\set\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?#storage#volume#{74a4ebdb-f4e7-11df-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-
806e6f6e6963}#0000020d3a1e800#{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}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM/system/currentcontrolset/control/deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{a62f2240-e41e-11e4-a6ae-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\
94f2-00a0c91efb8b}\##?#storage#volume#{a62f2240-e41e-11e4-a6ae-
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
806e6f6e6963}#00000000000000#{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}#00000000000007e00#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\device 94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-806e6f6e6963}#000000075343e000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
                                                                    HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
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\
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
806e6f6e6963}#00000020f3026800#{53f5630d-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#{e29ac6c3-7037-11de-816d-806e6f6e6963}#000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
                                                                  HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens~key: HKLMNsystem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\with a current control deviceclasses \{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\with a current control deviced \{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\with a current control 
806e6f6e6963\#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLMN-system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#;?#storage#volume#{f1c1ea40-e477-11e4-9632-
806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLMNsystem\currentcontrol\set\control\deviceclasses\{53f5630d-b6bf-11d 94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot1#{53f5630d-b6bf-11d0-94f2-
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceciasses\קיבוים - ויטנים - שניסטים ברניכן ארביים ברנים ארביים ווארבים ארביים ברנים ווארבים ארביים ברנים ברנ
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Opens kev:
Opens key: nklm/system/currentcontrolset/control/devicetlasses/(3)150300-0601-1100
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-
                                                                     HKLM \verb|\system| current control \verb|\system| contro
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d 94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f5630d-b6bf-11d0-94f2-
                                                                     00a0c91efb8b}
                                                                      HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f5630d-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-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6b
00a0c91efb8b}
                                                                     HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Opens kev:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2
00a0c91efb8b}
HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\\537563Ud-pbbT-iiu
94f2-00a0c91efb8b\\##?#storage#volumesnapshot#harddiskvolumesnapshot8#\\\53f5630d-b6bf-11d0-94f2-
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Opens key:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
    Opens kev:
94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\uevileclasscs\\( \) 94f2-00a0c91efb8b\\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}\\\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\\ 5b45201d-f2f2-4f3b-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e6102&ev_02#4&1fc3087&0&28f0#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b
85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&2e5a831d&0&28f0#{5b45201d-
                                                                     HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
 f2f2-4f3b-85bb-30ff1f953599}
```

```
Opens key:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
f2f2-4f3b-85bb-30ff1f953599}
                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#
                                   oot#umbus#0000#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}
  Opens key:
                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
32c86e1ba19f}\#\control
  Onens key
                                    HKI M\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
bcf7-00aa00b7b32a}
Opens key: HKLM\system\currentcontrolset\control\ueviteilasss\\.______bcf7-00aa00b7b32a}\##?#acpi#pnp0c0a##{72631e54-78a4-11d0-bcf7-00aa00b7b32a}\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f72a537-0000f8753ed1}\\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-
                                    0000f8753ed1}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
  Opens key:
h7df-24c5d8a8cch83
  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 key:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}
  Opens kev:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2fab8e39&0&12345678&06&05#{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}
Opens key:
bc8c-00a0c91405dd}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Opens kev:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
bc8c-00a0c91405dd}\##?#acpi#pnp0303#4&1d401fb5&0#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co101#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c-
00a0c91405dd}
  Opens kev:
                                    HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
 bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&0000#{884b96c3-56ef-11d1-bc8c-
00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\##?#root#rdp_kbd#0000#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
  Opens key:
af1f-0000f800845c}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
  Opens key:
af1f-0000f800845c}\##?#acpi#pnp0400#481d401fb580#{97f76ef0-f883-11d0-af1f-0000f800845c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\97fadb10-4e33-40ae
Opens key:
359c-8bef029dbdd0}
_x3220__@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
 _intel(r)_xeon(r)_cpu_
                                    HKLM\svstem\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#_3#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-359c-8bef029dbdd0}\\#;?#acpi#genuineintel_-_x86_family_6_model_15_-
                                             x3220 @ 2.40ghz# 4#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
 _intel(r)_xeon(r)_cpu_
Opens key:
901f-00c04fb951ed}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-
  Opens key
                                    HKI M\system\currentcontrolset\control\deviceclasses\{a5dchf10-6530-11d2-
 901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34a9bc#{a5dcbf10-6530-11d2-901f-
00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#fac72212e15ea84#{a5dcbf10-6530-11d2-901f-
00c04fb951ed}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}
Openskey: 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\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&27c84f55&0&00e4#{ad498944-
 762f-11d0-8dcb-00c04fc3358c}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens key:
8dcb-00c04fc3358c}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad49894
 762f-11d0-8dcb-00c04fc3358c}
                                   HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens kev:
8dcb-00c04fc3358c}\##?#root#*isatap#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}
8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\\#?#root#ms_l2tpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
\label{lem:openskey: HKLMN-system-current} Openskey: $$HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-currentcontrol-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-set-control-se
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens key:
HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens key
8dcb-00c04fc3358c}\##?#root#ms_ndiswanipv#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLMNsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
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: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#ms_sstpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens key:
8dcb-00c04fc3358c}\##?#root#system#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens key:
8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-b42b-00805fc1270e}#asyncmac#
8dcb-00c04fc3358c}
  Opens key
                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}
  Opens key:
                                    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}
HKI M\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
7515-4c03-82e6-71a87abac361}
Opens key: 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}
82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
```

```
82e6-71a87abac361}\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}
HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Opens key
82e6-71a87abac361}\##?#
                                           oot#ms_l2tpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
   Opens key:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_ndiswanip#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                             HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms ndiswanipy6#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLMIsystem\currentcontrolset\control\deviceclasses\{cac88484-7515-82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
  Opens key:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_sstpminiport#0000#(cac88484-7515-4c03-82e6-71a87abac361)
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361\} \\ \text{##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}} \\ \text{#asyncmac\#{cac88484-7515-4c03-1270e}} \\ \text{#asyncmac\text{cac88484-7515-4c03-1270e}} \\ \text{#asyncmac\text{cac88484-7515-4c03-1270e}} \\ \text{#asyncmac\text{cac88484-7515-4c03-1270e}} \\ \text{#asyncmac\text{cac88484-7515-4c03-1270e}} \\ \text{#asyncmac\text{cac88484-7515-4c03-1270e}} \\ \text{#asyncmac\text{cac88484-7516-4c03-1270e}} 
82e6-71a87abac361}
  Opens kev:
                                             HKLM\svstem\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
ac88-96b894c191e2}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
  Opens key:
ac88-96b894c191e2}\##?#acpi#pnp0c0a#0#{e849804e-c719-43d8-ac88-96b894c191e2}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
Opens key:
bcaa-942b18988098}
HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
usb#root_hub#4&22939226&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
Opens key:
bcaa-942b18988098}\##?#i
  Opens key
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
bcaa-942b18988098}\##?#usb#root_hub#4&2a2237a3&0#{ed8cf6b1-62d5-4597-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}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-
Opens key:
8815-00a0c906bed8}
Opens key: HKLM\\system\currentcontrol\set\control\deviceclasses\\{f18a0e88-8815-00a0c906bed8}\\##?#usb#root_hub#4&13571ab5&0#\{f18a0e88-c30c-11d0-8815-00a0c906bed8}
                                            HKLM \setminus system \setminus current control \setminus device classes \setminus \{f18a0e88-c30c-11d0e91e \} = \{f18a0e86-c30c-11d0e91e \} = \{f18a
Opens key:
8815-00a0c906bed8}\##
                                      HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
  Opens key:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906l
                                     #?#usb#root_hub#4&22939226&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
   Opens key:
8815-00a0c906bed8}\##?#usb#root_hub#4&24693ec3&0#tf18a0e88-c30c-11d0-8815-00a0c906bed8}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\\system\currentcontrol\set\control\deviceclasses\\{f18a0e88-8815-00a0c906bed8}\\##?#usb#root_hub#4&395eaf14&0#\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\\
                                             HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub20#4&211f73e0&0#\\f18a0e88-c30c-11d0-8815-00a0c906bed8\
   Opens key
                                            HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub20#4&305beb51&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
   Opens kev:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}
   Opens key
                                            HKI M\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
   Opens key
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdl1findoidinfo
Opens key: HKLM\software\microso
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
   Opens key:
                                             HKLM\system\currentcontrolset\control\mui\stringcachesettings
   Opens key:
                                             HKCU\software\classes\local settings\muicache\27\52c64b7e
                                             HKCU\software\classes\local settings\muicache
   Opens key
   Opens key:
Opens key
                                            HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
08002be10318}
                                            HKLM\system\currentcontrolset\services\umbus
   Opens key:
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
   Opens key
0\cryptdl1findoidinfo\1.3.6.1.4.1.311.47.1.1!7
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7
  Opens kev
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
Opens key: httlM\software\microsoft\cryptography\oid\encodingtype

HKLM\software\microsoft\cryptography\oid\encodingtype
Opens key.

HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllencodeobjectex
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex
                                            {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus oid \setminus encoding type}
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.1.1
                                            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
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.3
                                            HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.4
   Opens key:
                                            HKLM\software\microsoft\windows\currentversion\setup
   Opens key:
                                            HKLM\system\currentcontrolset\control\print
                                            HKCR\clsid
   Opens key:
   Opens key
                                            HKLM\software\policies\microsoft\windows nt\printers
   Opens key:
                                             HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
   Opens key:
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
08002be10318}\0007\linkage
   Opens key:
                                            HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
  Opens key
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Opens key:

08002be10318}\0006\linkage

Onens kev: HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
                                            HKCR\appid\vssvc.exe
HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
   Opens key:
   Opens key:
                                            HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\treatas
                                             HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid
   Opens key
```

```
Opens key
                                                 HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprocserver32
                                                 \label{eq:hkkr} HKKR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\) inprochandler 32 HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\) inprochandler 32 HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\) in prochandler 32 HKCR\clsid\e579ab5f-1cc4-44b4-bed9-de0991ff0623\}\) in prochandler 32 HKCR\clsid\
   Opens key:
   Opens key:
   Opens key:
                                                 HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
   Opens key:
                                                HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\treatas
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid
   Opens key:
                                                 HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprocserver32
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler32
   Opens key:
   Opens key:
   Opens key
                                                 HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler
   Opens key:
                                                 HKLM\system\currentcontrolset\services\vss\settings
   Opens key:
                                                 HKLM\svstem\currentcontrolset\services\vss\diag
                                                 HKLM\\system\currentcontrolset\services\vss\diag\registry writer
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
   Opens key:
   Opens key:
   Opens key
                                                 HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
                                                HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\procerver32
   Opens key:
   Opens key:
                                                 HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
   Opens key:
   Opens key:
   Opens key:
                                                 HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
                                                 HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
   Opens key:
                                                 HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\progid
                                                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
   Opens key:
   Opens key:
   Opens key:
                                                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler
HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
                                                 HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32
   Opens key:
                                                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
   Opens key:
   Opens key:
   Opens key:
                                                 HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\progid
HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
   Opens key:
                                                 HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
                                                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler
HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}
    Opens key:
   Opens key:
   Opens key:
                                                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}
HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
   Opens key:
                                                 HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid
                                                HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32
HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler32
   Opens key:
   Opens key:
   Opens key:
Opens key:
                                                 HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler
HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}
                                                 HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
   Opens key:
                                                 HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
HKLM\system\currentcontrolset\services\vss\diag\asr writer
    Opens key:
   Opens key
   Opens key
                                                 {\tt HKLM \ } system \verb| current control set \verb| services \verb| vss \verb| diag \verb| shadow copy optimization \\
writer
  Opens key:
                                                 HKCR\interface\{0000000c-0000-0000-c000-00000000046}
                                                 HKCR\interface\{0000000c-0000-0000-c000-00000000046}\proxystubclsid32
    Opens key:
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\sychost\wersycgroup
  Opens key:
Opens key:
                                                 HKLM\system\currentcontrolset\services\wersvc\HKLM\system\currentcontrolset\services\wersvc\parameters
   Opens key:
                                                \label{thm:loss} HKLM \software \microsoft \windows error reporting \\ HKLM \software \microsoft \windows nt \current \version \svchost \mbox{\schost} \mbo
   Opens key:
   Opens key:
                                                 HKLM\svstem\currentcontrolset\services\stisvc
   Opens key:
                                                 HKLM\system\currentcontrolset\services\stisvc\parameters
HKLM\system\currentcontrolset\control\stillimage\trace
   Opens key:
   Opens key:
                                                 HKLM\system\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:
                                                HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\treatas
HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\progid
   Opens key:
   Opens key:
                                                 HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprocserver32
                                                 HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler32
   Opens key:
   Opens key:
                                                 HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler
   Opens key:
                                                HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\treatas
   Opens key:
   Opens key:
                                                 HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\progid
HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprocserver32
   Opens key:
                                                 HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler32
   Opens key:
   Opens key:
                                                 HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler
HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
   Opens key:
   Opens key:
                                                HKLM\system\currentcontrolset\control\stillimage\fakedevices HKLM\system\currentcontrolset\control\stillimage\mscdevicelist
   Opens key:
   Opens kev:
                                                 HKLM\svstem\currentcontrolset\control\stillimage
    Opens key:
                                                 HKLM\system\currentcontrolset\control\stillimage\events
                                                 HKLM\system\currentcontrolset\control\stillimage\events\connected
   Opens key:
Opens key: 
HKLM\system\currentcontrolset\control\stillimage\events\connected\{38f8a702-36bb-4a68-80e6
d4966b9bb7183
                                                 HKLM \verb|\system| current controls et \verb|\control| still image \verb|\events| disconnected |
   Opens key:
                                                 HKLM\system\currentcontrolset\control\stillimage\events\emailimage
   Opens key:
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
   Opens key:
                                                 HKLM\system\currentcontrolset\control\stillimage\events\faximage
   Opens kev:
759eb35cdf9a}
   Opens kev:
                                                 HKLM\system\currentcontrolset\control\stillimage\events\printimage
    Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
                                                 HKLM\system\currentcontrolset\control\stillimage\events\scanbutton
   Opens key:
Opens~key: \\ HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6}
d4966b9bb718}
   Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f223
   Opens key:
HKLM\system\currentcontrol\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
   Opens key:
\label{thm:hkkin} HKLinvsystem \current control still image \events \scan button \eabbd 70d-a 25f-4e 90-96a 4-7105 fd 3b 53b 1\}
                                                 HKLM\svstem\currentcontrolset\control\stillimage\events\stiproxvevent
   Opens kev:
                                                HKLM\system\currentcontrolset\control\stillimage\serversettings
HKLM\system\currentcontrolset\services\nativewifip
   Opens key:
   Opens key:
   Opens key:
                                                 HKLM\system\currentcontrolset\services\nativewifip\enum
   Opens key:
                                                 HKLM\system\currentcontrolset\enum\root
   Opens key:
                                                 HKLM\svstem\currentcontrolset\enum\root\legacv nativewifip\0000
                                                 HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-
   Opens key
```

```
0000f8753ed13
Opens key:
08002be10318}
                                                                Opens key
                                                                HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
08002be10318}\{e475cf9a-
                                                             -60cd-4439-a75f-0079ce0e18a1}\ndi
   Opens key:
                                                                HKLM\svstem\currentcontrolset\services\nativewifip\parameters
                                                               HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000
     Opens key:
     Opens key:
    Opens key:
                                                                HKLM\svstem\currentcontrolset\services\ndisuio
Opens key: H
08002be10318}\0005\linkage
                                                                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                                                HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
     Opens key:
                                                                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Opens key
08002be10318}\0008\linkage
    Opens key:
                                                                HKLM\system\currentcontrolset\services\ndisuio\enum
                                                               HKLM\xsystem\currentcontrolset\enum\noot\legacy\_ndisuio\xsuperlines of the months of
    Opens key:
     Opens key:
    Opens key
Opens key: 08002be10318}\0000\linkage Opens key: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
                                                                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Opens key:

08002be10318}\0003\linkage

Opens key: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
                                                                08002be10318}\0004\linkage
   Opens key:
                                                               HKLM\system\currentcontrolset\enum\root\ms 12tpminiport\0000
                                                                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\linkage
                                                               HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
Opens key:
08002be10318}\0001\linkage
                                                                HKLM\system\currentcontrolset\services\nnetsecl\paramete
     Opens key:
    Opens key:
                                                                HKLM\system\currentcontrolset\enum\root\*teredo\0000
     Opens key
                                                                08002be10318}\0011\linkage
                                                                HKLM\svstem\currentcontrolset\enum\root\*isatap\0000
   Opens key:
Opens key: HI
08002be10318}\0009\linkage
                                                                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
Opens key:
                                                               HKLM\system\currentcontrolset\control\diagnostics\performance
HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger
     Opens key:
                                                                HKLM\system\currentcontrolset\services\spldi
                                                                HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
    Opens key
00805fc1270e}\asyncmac
    Opens key:
                                                                HKLM\system\currentcontrolset\enum\root\system\0000
    Opens key
                                                                HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac\properties
                                                               HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
    Opens key:
00805fc1270e}\asyncmac\properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}
Opens key: HKLM\system\currentcontrolset\hardware profiles\current
    Opens key:
                                                                HKLM\svstem\currentcontrolset\hardware profiles\0001
                                                                HKLM\system\currentcontrolset\hardware
profiles\0001\svstem\currentcontrolset
Opens key: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\enum
    Onens key
                                                               HKLM \ system \ current controls et \ enum \ sw \ \{eeab 7790-c514-11d1-b42b-c514-c11d1-b42b-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-c514-c11d1-
00805fc1270e}\asyncmac\control
    Opens key
                                                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}
   Opens key:
                                                                HKLM\system\currentcontrolset\services\asyncmac
    Opens key
                                                                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\properties
                                                                HKLM\svstem\currentcontrolset\services\asvncmac\enum
    Opens kev:
     Opens key:
                                                               HKLM\system\currentcontrolset\enum\root\legacy_asyncmac
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Opens key:
Opens key:

08002be10318}\0010\linkage

Onens kev: HKLM\system\currentcontrolset\control\storage
                                                                \label{local-equation} HKLM\system\currentcontrolset\control\storage\{cac88484-7515-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-4c03-82e6-
71a87abac361}
Opens key: HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab7790-c514-11d1-b42b-ceab
Opens key: HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-00805fc1270e}\asyncmac\properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000006
   Opens key:
Opens key:
                                                               HKLM\system\currentcontrolset\services\ndiswan
HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asvncmac\properties\{3ab22e31-8264-4b4e-9af5-a8d2d8e33e62}
     Opens key:
                                                                HKLM\system\currentcontrolset\services\ndis\iftypes\23\0
    Opens key:
                                                                HKLM\system\currentcontrolset\control\storage\{ad498944-762f-11d0-8dcb-
00c04fc3358c}
    Opens key:
                                                                HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}\#
                                                                HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Opens key:
8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0
8dcb-00c04fc3358c}\#{e2f8a220-af88-446c-9a55-453e58dd3a33}
    Opens kev:
                                                               {\tt HKLM \ } system \verb|\ current control \verb|\ cryptography \verb|\ providers| \\
                                                                HKLM\system\currentcontrolset\control\cryptography\configuration
    Oueries value
                                                                HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\:
                                                               HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
     Oueries value:
                                                                HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                               HKCU\control panel\desktop[preferreduilanguages]
HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
     Queries value:
     Queries value:
     Oueries value:
 HKLM\software\microsoft
                                                            \windows\currentversion\sidebyside[preferexternalmanifest]
    Oueries value:
                                                                HKLM\svstem\currentcontrolset\control\nls\sorting\versions[]
     Queries value:
                                                                HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                                                HKLM\software\microsoft\rpc[maxrpcsize]
     Queries value:
     Oueries value
 HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                                               HKLM\system\setup[oobeinprogress]
HKLM\system\setup[systemsetupinprogress]
HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Oueries value:
     Queries value:
     Queries value:
                                                               Oueries value
     Queries value:
    Oueries value:
                                                                HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[alg]
                                                               HKLM\system\currentcontrolset\control\cmf\config[system]
HKLM\software\microsoft\windows
     Oueries value
     Queries value:
nt\currentversion\windows[loadappinit dlls]
                                                                HKLM\software\microsoft\ole[pageallocatorusesystemheap]
     Queries value
```

```
Oueries value:
                                                                   HKLM\software\microsoft\ole[pageallocatorsvstemheapisprivate]
                                                                   HKLM\software\microsoft\com3[com+enabled]
HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
      Queries value
     Queries value:
                                                                   \label{thm:hklm:software} HKLM \software \microsoft \ole[defaultaccesspermission] \\ HKLM \software \microsoft \ole[defaultaccesspermission] \\
     Oueries value
     Queries value
     Oueries value
                                                                   HKLM\system\currentcontrolset\control\lsa[evervoneincludesanonymous]
     Queries value
                                                                   HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wicrosoft \label{lem:hklm} software \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} wicrosoft \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hkklm} \
cryptographic provider[type]
     Oueries value
                                                                   HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 cryptographic provider[image path]
                                                                  HKLM\system\currentcontrolset\control\session
    Oueries value
 manager[safeprocesssearchmode]
                                                                  HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Queries value:
                                                                  HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
     Oueries value
     Queries value
    Oueries value:
Queries Value.

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

Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                                                  HKLM\software\microsoft\cryptography[machineguid]
HKCR\interface\{00000134-0000-0000-0000-00000000046}\proxystubclsid32[]
     Oueries value
     Queries value
    Oueries value:
                                                                   HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                                                                  HKLM\software\microsoft\rpc\extensions[remoterpcdl1]
HKLM\software\microsoft\sqmclient\windows\disabledprocesses[bca9f854]
      Queries value:
     Queries value:
     Oueries value
 HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
    Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} icrosoft \end{tabular} sqmclient \end{tabular} windows \end{tabular} disable dessions \end{tabular} global session \end{tabular}
                                                                   HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:
    Queries value:
Queries value:
                                                                  HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
HKLM\software\microsoft\msdtc\tracing\sources[trace_misc]
                                                                  HKLM\software\microsoft\msdtc\tracing\sources[trace_rm]
HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
    Oueries value:
      Queries value:
     Queries value:
    Queries 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]
HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
HKLM\software\microsoft\msdtc\tracing\sources[trace_cluster]
    Oueries value:
      Queries value:
     Queries value:
    Queries 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_trp]
HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
HKLM\software\microsoft\msdtc\tracing\sources[trace_bg]
HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
    Oueries value:
      Queries value:
     Oueries value:
    Queries value:
Queries value:
                                                                   \label{thm:local-hammer} HKLM \software \subseteq \ ktmrm] \\ HKLM \software \subseteq \ ktmrm] \subseteq \ hklm \subseteq \
    Oueries value:
      Queries value:
                                                                   HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon] HKLM\software\microsoft\msdtc\tracing\sources[trace_tm] HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
     Oueries value:
     Queries value:
     Queries value:
                                                                  Oueries value:
      Queries value:
                                                                   \label{thm:local_hammon_hammon} HKLM \software \microsoft \mbox{$\mbox{$m$icrosoft$ $\mbox{$m$icrosoft$ 
     Oueries value:
     Queries value:
     Queries value
HKLM\software\microsoft\msdtc[snapshotprefertransactionstimeoutduringbackup]
                                                                   HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
     Queries value:
    Oueries value:
                                                                   HKLM\software\microsoft\windows
nt\currentversion\tracing\msdft\misc[disabletracing]
Queries value: HKLM\software\microsoft\msdtc[disableterminationonheapcorruption]
                                                                  HKLM\software\microsoft\msdtc[sysprepinprogress]
HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
     Oueries value
     Queries value:
                                                                  HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\description[]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\description[]
HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5\description[]
     Oueries value:
     Queries value:
    Queries value:
                                                                    HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\description[]
     Oueries value
     Queries value:
                                                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\description[]
     Oueries value:
                                                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid[]
     Queries value:
                                                                   HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\host[]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\clsid[]
     Queries value
     Oueries value
                                                                    HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
      Queries value:
                                                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\protocol[]
                                                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\endpoint[]
     Oueries value:
Queries value: HKCR\cid.local\d
782ab52d45ed\customproperties\log\size[]
                                                                    HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
    Queries value:
Queries value:
                                                                  HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib]
     Oueries value:
                                                                   HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
      Queries value
                                                                   HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
    Queries value:
    Queries value:
Queries value:
                                                                   HKLM\software\microsoft\msdtc\security[accountname] HKLM\software\microsoft\msdtc\security[networkdtcaccess]
                                                                  HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
     Oueries value:
     Queries value:
     Queries value:
    Queries value:
Queries value:
                                                                   HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
     Oueries value:
                                                                    HKLM\software\microsoft\msdtc\security[xatransactions]
                                                                  HKLM\software\microsoft\msdtc\security[lutransactions]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
     Queries value
    Oueries value
782ab52d45ed\customprop
                                                                 rties\log\path[]
                                                                   HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-
    Queries value
8bd7-da8f1a74051a1
                                                                    HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxbuffers]
    Oueries value:
                                                                  HKLM\software\microsoft\window
 nt\currentversion\tracing\msdtc\loggingoptions[minbuffers]
    Oueries value:
                                                                  HKLM\software\microsoft\windows
\label{lem:ntcurrentversion} $$ ntcurrentversion\tracing\msdtc\loggingoptions[buffersize] $$ Queries value: $$ HKLM\software\microsoft\windows $$ $$
\label{lem:ntcurrent} $$nt`currentversion`tracing`msdtc\loggingoptions[maxfilesize] $$Queries\ value: $$HKLM\system\currentcontrolset\control\timezoneinformation[bias]$$
    Oueries value:
                                                                   HKLM\system\currentcontrolset\control\timezoneinformation[standardname]
                                                                  HKLM\system\currentcontrolset\control\timezoneinformation[standardbias] HKLM\system\currentcontrolset\control\timezoneinformation[standardstart]
     Queries value:
     Queries value:
     Oueries value
                                                                    HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
    Oueries value:
                                                                   HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[uniqueid]
    Oueries value:
                                                                  HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[active]
    Oueries value:
                                                                  HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[level]
```

```
Oueries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[controlflags]
Queries value: HKLM\software\microsoft\windows
Queries value: hKLM\software\microsoft\windows

Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
   Oueries value
                                                      HKIM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
                                                      HKLM\system\currentcontrolset\control\wmi\security[e80aa9fe-913d-4ede-
   Oueries value:
af58-73e332dcac8d]
                                                       HKLM\software\microsoft\msdtc[dtcmaxsessions]
   Queries value:
                                                      \label{thm:hammon} HKLM \software \microsoft \mbox{$\mathsf{MKLM}$ software \microsoft \mbox{$\mathsf{MKLM}$ software \mbox{$\mathsf{MKLM
    Oueries value
    Queries value
   Oueries value:
                                                      HKLM\software\microsoft\msdtc[mincheckpointinterval]
                                                      HKLM\software\microsoft\msdtc[maxcheckpointinterval]
HKLM\software\microsoft\msdtc[waitforallxabranchprepares]
    Queries value:
    Queries value:
                                                      HKLM\software\microsoft\msdtc\security[snapshotsecuritydisabled]
HKLM\software\microsoft\msdtc[servertcpport]
    Oueries value
    Queries value
   Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion[currentversion]
                                                      HKLM\software\microsoft\msdtc[cmcancelrpcafter]
HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
    Queries value:
    Queries value:
                                                      HKLM\software\microsoft\msdtc[cmmaxidlepings]
HKLM\software\microsoft\msdtc[cmpingfreqsecs]
    Oueries value:
    Queries value
   Oueries value:
                                                       HKLM\software\microsoft\msdtc[cmverbose]
                                                      HKLM\software\microsoft\msdtc[rpcqoscapabilities]
HKLM\software\microsoft\msdtc[rpcqosidentity]
    Queries value:
    Queries value:
                                                      HKLM\software\microsoft\msdtc[rpcauthnsvc]
HKLM\software\microsoft\msdtc[numcccimhistoryentries]
    Oueries value:
    Queries value
   Oueries value:
                                                       HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\svcid[]
                                                      HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\host[]
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\clsid[]
    Queries value:
    Queries value:
   Queries value:
Queries value:
                                                      HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[] HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\protocol[]
                                                       HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\endpoint[]
   Oueries value:
                                                      HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
    Queries value:
    Queries value:
    Queries value:
                                                      HKLM\software\microsoft\msdtc[notracking]
HKLM\software\microsoft\rpc\securityservice[9]
    Queries value
   Oueries value:
 Oueries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \current control \end{tabular} extension config \spicli [check signature routine] \end{tabular}
   Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
    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\control\lsa\sspicache\credssp.dll[rpcid]
     Queries value:
                                                       HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
    Oueries value:
                                                      HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
    Queries value
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
   Oueries value
 HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
    Oueries value:
    Queries value:
                                                      HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:
                                                      HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\svcid[]
    Oueries value
                                                      HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\nost[]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\nost[]
    Queries value:
    Oueries value:
    Queries value:
                                                      \label{eq:hkcr} HKCR\svcid.local\10366d42-c04e-11d1-b1c0-00c04fc2f3eftdefaultprovider[]\\ HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol[]
   Queries value:
    Oueries value
                                                       HKCR\cid local\199661d8-979c-4ebb-9e3e-a23014be3f1a\endpoint[]
    Queries value:
                                                       HKLM\software\microsoft\msdtc[overridetiphostname]
                                                      HKLM\software\microsoft\msdtc[shared_memory_mutex_timeout]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\svcid[]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\host[]
    Oueries value:
    Queries value:
   Queries value:
    Oueries value
                                                       HKCR\cid local\81a3a129-619d-4d5f-a782-28d960ea489d\clsid[]
    Queries value:
                                                       HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
                                                      HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\protocol[]
    Oueries value:
    Queries value:
                                                      HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\endpoint[]
HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
    Queries value:
                                                      HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
HKLM\software\microsoft\msdtc[transactionbridge]
    Oueries value:
    Queries value:
    Oueries value:
                                                       HKLM\software\microsoft\msdtc[logwarnenabled]
    Queries value
                                                      HKLM\software\microsoft\msdtc[suppressduplicateduration]
HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
    Queries value:
                                                      HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4\\progid[]
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4\}[]
    Oueries value:
    Queries value
   Oueries value
                                                      HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocse
                                                      er32[inprocserver32]
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
   Queries value
    Oueries value
                                                      HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
                                                      HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
   Oueries value
                                                       HKLM\software\microsoft\msdtc[supportns]
    Queries value
                                                      HKU\.default\control panel\desktop[preferreduilanguages]
    Oueries value:
Queries value: HKU\.default\control panel\desktop\muicached[machinepreferreduilanguages]
   Oueries value
                                                      HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[ui0detect]
                                                      HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
   Oueries value:
OfbS8b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
                                                      HKLM\system\currentcontrolset\control\nls\localef0000004091
    Oueries value:
    Queries value
                                                       HKLM\system\currentcontrolset\control\nls\language groups[1]
   Oueries value
                                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore v1.0[datafilepath]
    Queries value:
                                                      HKLM\software\microsoft\window
\label{lem:ntcurrent} $$nt` currentversion\languagepack\surrogatefallback[plane1] $$Queries\value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] $$
   Oueries value
                                                      HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback[plane3]
   Oueries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
    Oueries value
                                                      HKLM\software\microsoft\window
```

```
HKLM\software\microsoft\window
      Queries value
nt\currentversion\languagepack\surrogatefallback[plane8]
    Oueries value
                                                                             HKLM\software\microsoft\windows
nt\currentversion\langu
                                                                         agepack\surrogatefallback[plane9]
    Oueries value:
                                                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                                                                             HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
     Queries value:
                                                                             HKLM\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback[plane13]
     Oueries value
                                                                             HKI M\software\microsoft\window
nt\currentversion\langu
                                                                         agepack\surrogatefallback[plane14]
    Oueries value:
                                                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\svchost[localservicepeernet]
      Queries value
                                                                              HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
     Queries value:
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain]
     Oueries value:
                                                                             HKLM\software\microsoft\windows
 nt\currentversion\winlogon[userenvdebuglevel]
                                                                             HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
     Queries value:
      Oueries value:
                                                                             HKLM\software\policies\microsoft\peernet[disabled]
      Queries value
HKLM\system\currentcontrolset\services\p2pimsyc\parameters[servicedllunloadonstop]
      Queries value:
                                                                             HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll]
      Queries value:
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]

Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
     Queries value:
     Oueries value:
                                                                             HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
       Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
      Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
     Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
      Oueries value
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000001\packedcatalogitem]
      Queries 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
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000005packedcatalogiteml
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000fpackedcatalogitem]
      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\spaces\parameters\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog\_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog9\catalog_entries\protocol\_catalog_entries\protocol\_catalog_entries\protocol\_catalog_entries\protocol\_catalog_ent
     Oueries value
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000011[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\current control set\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\commont{1}{0}000000000013\\ [packed catalog item]
     Oueries value:
Queries value:
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \common 000000000015 \cite{thmoson} \parameters \paramete
      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
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 [serial\_access\_num]
     Queries value:
Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 000000000001 [library path]
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001fdisplaystring7
      Queries value:
Oueries value:
Oueries value
Queries value
\label{local-parameters} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog \catalog\_entries \colonormal \current \curre
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[version]
      Queries value:
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo]
    Oueries value
HKL\\ M\system\current control set\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[providerid]
      Queries value:
Oueries value
HKLM \label{thm:mass} \label{thm:mass} HKLM \label{thm:mass} \label{thm:mass} HKLM \label{thm:mass} \label{thm:mass} \label{thm:mass} HKLM \label{thm:mass} \
     Oueries value
```

nt\currentversion\languagepack\surrogatefallback[plane7]

```
Oueries value
Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000002[providerinfo]
   Oueries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ \ 0000000000003 [library path]
   Oueries value
Oueries value:
Queries value:
\label{local-parameters} HKLM \system \current controlset \services \winsock 2 \parameters \names pace\_catalog5 \catalog\_entries \0000000000003 \[address family] \queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003fsupportednamespace1
    Queries value:
HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace\_catalog \\ 5 \\ catalog\_entries \\ 0000000000003 \\ [enabled]
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
   Oueries value:
Queries value:
\label{local-prop} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000000003[providerinfo]\ Queries\value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004flibrarvpath1
    Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\common000000004[displaystring]
   Oueries value
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004\providerid7
   Oueries value:
Queries value:
\label{prop:hklm} HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names \n
   Queries value:
Queries value
HKL\\ M\system\current control set\services \winsock 2 parameters \namespace\_catalog 5 \catalog\_entries \na
    Oueries value:
Oueries value:
Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005fproviderid1
    Queries value:
Oueries value:
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\space]
   Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005fversion1
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000005fstoresserviceclassinfol
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
   Oueries value
Oueries value:
HKL\\ M (system \current control set \services \winsock 2 \parameters \nowed by a catalog 5 \catalog\_entries \nowed by a catalog 5 \catalog 5 \catalog
   Queries value:
HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ \ namespace\_catalog \ 5 \ \ catalog\_entries \ \ \ 0000000000006 \ [providerid]
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006faddressfamilv1
    Queries value:
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\space]
   Oueries value
Oueries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
    Queries 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]
                                                       HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6[winsock 2.0 provider id]
   Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
    Oueries value
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
   Oueries value:
\label{thm:local_hklm} \begin{tabular}{ll} HKLM \begin{tabular}{ll} HKLM \begin{tabular}{ll} System \begin{tabular}{ll} Color & Colo
c19ce8a73253}[enabledhcp]
Queries 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:
\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
   Oueries value:
HKLMNsystem \current control set \services \tcpip\parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19c8a73253\} [dhcpdomain]
   Oueries value
```

c19ce8a73253}[dhcpv6domain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
 Queries value:
\label{local-bound} HKLM\system\currentcontrolset\services\tcpip\parameters\tinterfaces\eq29ac6c2-7037-11de-816d-806e6f6e6963\\\[registrationenabled]
 Oueries value:
806e6f6e6963}[registeradaptername]
 Oueries value
```

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain]

Queries value

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpdomain]

HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Oueries value: HKLM\software\microsoft\samclient[machineid] Queries 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: linklocal\linklocal\_ff00::%11/8[disablemulticastpublish]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-

linklocal\linklocal\_ff00::%11/8[disablemulticastsearch]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-

Queries value: nkm\software\microsoft\mindows\mi\currentversion\peernet\pnrp\ipvo-linklocal\finklocal\_ff00::\mildows\microsoft\mindows\microsoft\mindows\microsoft\mindows\microsoft\mindows\microsoft\mindows\microsoft\mindows\microsoft\mindows\microsoft\mindows\microsoft\mindows\mindow\mindows\mindows\mindows\mindows\mindows\mindows\mindows\mindows\mindows\mindows\

Oueries value:

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

 $Queries\ value: \\ HKLM\ value: \\ H$ a03a-e3ef65729f3d}[name]

Queries value:

a03a-e3ef65729f3d}[parentfolder]

Queries value:

a03a-e3ef65729f3d}[description]

Oueries value:

a03a-e3ef65729f3d}[relativepath1

Oueries value:

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

Queries value:

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

a03a-e3ef65729f3d}[localizedname]

Oueries value:

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

Oueries value:

a03a-e3ef65729f3d}[security]

Queries value:

a03a-e3ef65729f3d}[streamresource]

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

Queries value:

a03a-e3ef65729f3d}[localredirectonly]

Oueries value:

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

Oueries value:

a03a-e3ef65729f3d}[precreate]

Queries value:

a03a-e3ef65729f3d}[stream1

Queries value:

 $HKLM \label{eq:hkkk} Which is the statement of the stat$ a03a-e3ef65729f3d}[publishexpandedpath]

Queries value:

a03a-e3ef65729f3d}[attributes] Oueries value:

 $\label{lem:condition} White the description of th$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

HKLM\software\microsoft\windows nt\currentversion\profilelist[public] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
HKLM\software\microsoft\windows\currentversion[commonfilesdir]
HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)] Oueries value: Queries value: Queries value: Oueries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir] Oueries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir] Queries 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] Oueries value:

Queries value:

 $HKLM \label{eq:hkkk} Which is the statement of the stat$ 9afe-ea3317b67173}[category]

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

Queries value:

9afe-ea3317b67173}[parentfolder]

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}[description]

Queries value

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{5e6c858f-0e22-4760-164e1\} + \{5e6c858f-0e22-4660-164e1\} + \{5e6c858f-0e22-4660-164e1\} + \{5e6c858f-0e22-4660-164e1\} + \{5e6c858f-0e22-4660-1646$ 9afe-ea3317b67173}[relativepath]

9afe-ea3317b67173}[parsingname]

Queries value:

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

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \mbox{$microsoft$} \windows \current version \explorer \footnote{thm:local_hammon_hammo$ 9afe-ea3317b67173}[localizedname]

Oueries value:

 $\label{thm:continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \cite{thm:continuous} \end{substitute} $$ 100. \cite{thm:continuous} \cit$ 9afe-ea3317b67173}[icon]

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

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{5e6c858f-0e22-4760-164e1\} + \{5e6c858f-0e22-4660-164e1\} + \{5e6c858f-0e22-4660-164e1\} + \{5e6c858f-0e22-4660-164e1\} + \{5e6c858f-0e22-4660-1646$ 9afe-ea3317b67173}[streamresource]

Queries value:

9afe-ea3317b67173}[streamresourcetype]

Oueries value:

 $HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions|| \{5e6c858f-0e22-4760-9afe-ea3317b67173\}[local redirectonly] \} and the property of the$ 

Oueries value:

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

 $\label{lem:queries} Queries \ value: \\ HKLM\ valu$ 9afe-ea3317b67173}[precreate] Queries value:

9afe-ea3317b67173}[stream]

Queries value:

 $\label{local-prop} HKLM \normalisation which is the sum of the s$ 

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \mbox{$microsoft$} \windows \current version \explorer \folder descriptions \colored by the control of the control of$ 9afe-ea3317b67173}[attributes]

Queries value:

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

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-

9afe-ea3317b67173}[initfolderhandler]

Queries value: HKLM\system\c HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

Oueries value: HKLM\software\microsoft\cryptography\defaults\provider types\type

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

schannel cryptographic provider[type]

Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa

schannel cryptographic provider[image path]

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

Queries value:

a9dd-070d1d495d97}[name]

Oueries value:

 $HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[parentfolder]$ 

Oueries value

a9dd-070d1d495d97}[description]

Queries value:

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

 $\label{thm:local-equation} HKLM \software \mbox{$microsoft\windows\currentversion} \end{supplies} According to the content of the content o$ a9dd-070d1d495d97}[parsingname]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82 - fdc1 - 4dc3 - fdc1 - 4dc3 - fdc1 - 4dc3 - fdc1 - fd$ a9dd-070d1d495d97}[infotip]

Oueries value:

 $HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[localized name]$ 

a9dd-070d1d495d97}[icon]

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

a9dd-070d1d495d97}[security] Queries value:

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

a9dd-070d1d495d97}[streamresource] Oueries value:

a9dd-070d1d495d97}[streamresourcetype] Oueries value:

a9dd-070d1d495d97}[localredirectonlv1

Queries value:

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

a9dd-070d1d495d97}[roamable]

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

a9dd-070d1d495d97}[precreate]

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

a9dd-070d1d495d97}[stream]

Oueries value: 

a9dd-070d1d495d97}[publishexpandedpath] Oueries value:

 $\label{thm:condition} HKLM \software \mbox{$microsoft$} windows \current version \explorer \folder descriptions \folder \fol$ 

a9dd-070d1d495d97}[attributes]

Queries value:

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

a9dd-070d1d495d97}[foldertypeid]

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82 - fdc1 - 4dc3 - fdc1 - fd$ a9dd-070d1d495d97}[initfolderhandler]

Oueries value: HKLM\software\policies\microsoft\cryptography[forcekeyprotection] Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#?#umb#umb#1&841921d&0&printerbusenumerator#\65a9a6cf-64cd-480b-843e-32c86e1ba19f}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\#\control[linked] Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#\65a9a6cf-64cd-480b-843e-32c86e1ba19f}\control[referencecount] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-Oueries value: b082-00a0c91efb8b}[default] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-Queries value: h082-00a0c91efb8h}\##? #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-c130-11d2-Oueries value b082-00a0c91efb8b}\##?#pci#ven\_1000&dev\_0054&subsys\_1f091028&rev\_01#5&6373acf&0&400008#{2accfe60c130-11d2-b082-00a0c91efb8b}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082 00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance] Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&1#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2b082-00a0c91efb8b}\##?#pciide#idechannel#4&2d9c6e01&0&0#{2accfe60-c130-11d2-b082 00a0c91efb8b}[deviceinstance] Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#482f42c7138080#{2accfe60-c130-11d2-b082-00a0c91efb8b}[deviceinstance] Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{2acb082-00a0c91efb8b}\#?#pciide#idechannel#482f42c7138081#{2accfe60-c130-11d2-b082-HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-00a0c91efb8b}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-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] HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-bc8c-00a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&co102#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-bc8c-10a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&co102#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-bc8c-10a0c91405dd} 00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1bc8c-00a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&col02#6&1e20eb37&0&0001#{378de44c-56ef-11d1-bc8c 00a0c91405dd}[deviceinstance] HKLM\svstem\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] Oueries value HKI M\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1bc8c-00a0c91405dd}\##?#hid#vid\_14dd&pid\_1005&col03#6&1e20eb37&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd}[deviceinstance] Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[default] HKLM\svstem\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Oueries value: Queries value. 8a92-1e6861e6af27}\##?#pci#wen\_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] | The August 19 | The August 1 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&1&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Queries value: 8a92-1e6861e6af27}\##?#pci#ven\_6086&dev\_27ca&subsys\_01e61028&rev\_01#3&2411e6fe&0&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance] HKLM\svstem\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Oueries value: Queries value. ##?#pci#wen\_8086&dev\_27ca&subsys\_01e61028&rev\_01#3&2411e6fe&1&ea#{3abf6f2d-7tc4-462a-8a92-1e6861e6af27}[deviceinstance] Queries value: 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}[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] HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662b732-99a6111edc0b}[default] Queries value: HKI a5d6-28db04c10000}[default] HKLM\system\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-Queries value: 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-Oueries value: be5e-00a0c9062857}[default] HKLM\svstem\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-Oueries value: be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e 00a0c9062857}[deviceinstance] Oueries value: HKLM\svstem\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&1#{4afa3d53-74a7-11d0-be5e 00a0c9062857}[deviceinstance] Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-be5e-00a0c9062857}\\##?\acpi\#fixedbutton\#2\daba3ff\&2\#{4afa3d53-74a7-11d0-be5e-00a0c9062857}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}[default] Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-00111100030}\#;?#hid#vid\_14dd&pid\_1005&col01#6&1c83c2e&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}[deviceinstance] HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf- $88cb-001111000030\} \\ \text{\##?\#hid\#vid\_14dd\&pid\_1005\&col01\#6\&1e20eb37\&0\&0000\#\{4d1e55b2-f16f-11cf-88cb-1001111000030\}} \\ \text{\#pid\_1005\&col01\#6\&1e20eb37\&0\&0000\#\{4d1e55b2-f16f-11cf-88cb-1001111000030\}} \\ \text{\#pid\_1005\&col01\#6\&1e20eb37\&0\&0000\#\{4d1e55b2-f16f-11cf-88cb-1001111000030\}} \\ \text{\#pid\_1005\&col01\#6\&1e20eb37\&0\&0000\#\{4d1e55b2-f16f-11cf-88cb-1001111000030\}} \\ \text{\#pid\_1005\&col01\#6\&1e20eb37\&0\&0000\#\{4d1e55b2-f16f-11cf-88cb-100111000030\}} \\ \text{\#pid\_1005\&col01\#6\&1e20eb37\&0\&00000\#\{4d1e55b2-f16f-11cf-88cb-100111000030\}} \\ \text{\#pid\_1000030} \\ \text{\#p$ 001111000030}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-

88cb-001111000030}\##?#hid#vid\_14dd&pid\_1005&co102#6&1c83c2e&0&0001#{4d1e55b2-f16f-11cf-88cb-

88cb-001111000030}\##?#hid#vid\_14dd&pid\_1005&col02#6&1e20eb37&0&0001#{4d1e55b2-f16f-11cf-88cb

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

001111000030}[deviceinstance]

```
001111000030}[deviceinstance]
001111000030}[deviceinstance]
001111000030}[deviceinstance]
                                                                  HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
    Queries value:
94f2-00a0c91efb8b}[default]
Queries value: 94f2-00a0c91efb8b}\##?
                                                                  HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
_4.6.2.6_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-
                                                                 HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-
    Oueries value:
94f2-00a0c91efb8b}\##?
#ide#diskseagate
                                                                                                                                 5.7.4.5 #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#diskvbox_harddisk_
                                                                                                                                                        _#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\\ 53f56307-b6bf-11d0-94f2-00a0c91efb8b\\##?#scsi#disk&ven_dell&prod_virtual_disk#6&17b13437&0&00000#\\\ 53f56307-b6bf-
11d0-94f2-00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{53f56307-b6bf-11d0-
94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&3af2ddc5&0&000000#{53f56307-b6bf-
Tid0-94f2-00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}\\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
t10n_____1.02___#5&28836b8&0&0.0.0#{53f56308-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\{53f56308-b6bf-11d0-94f2-00a0c91efb8b\\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
                                                __1.05____#5&23a61b21&0&0.0.0#{53f56308-b6bf-11d0-94f2-
t10n
00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
| UUadus | Fishology | Leading | Company | Com
                                                                  HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
Queries value: HKLM\system\cur 94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
rom _____1.0 ______#5&394c0ad3&0&0.1.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
                                                               HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Oueries value:
94f2-00a0c91efb8b}[default]
                                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Oueries value:
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolse
94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
                                                                  HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
1.05 #$823a61b2180&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
                                                               HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value:
                                                              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                                                _______#5&394c0ad3&0&0.1.0#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\##?#storage#volume#\{69d250e0-6c18-11e3-b3bc-
806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
                                                                  HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
\text{\forage} \text{
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#00000000000000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLMNsystem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?\storage\volume\{74a4ebdb-f4e7-11df-aef6-806e6f6e6963\}\#000000075343e000\\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\[deviceinstance]
Queries \ value: \ HKLM\ system \ (current control set\ (control\ device classes\ \{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\}\ ) \ + \#?\#storage\#volume\#\{74a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-11df-aef6-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebdb-f4e7-44a4ebd
806e6f6e6963}#000001e628b7200#{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}#00000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value: httm://datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.com/datebub.
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLMN\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\##?#storage#volume#{a62f2240-e41e-11e4-a6ae-
806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\a62f2240-e41e-11e4-a6ae-
806e6f6e6963}#0000000000006500000#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\#r?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#00000000000000000004(53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
    Oueries value:
                                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000000075343e000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?#storage#volume#{e29ac6c3-7037-11de-816d-806ef6e6963}#0000001e628b7200#{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}#00000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
                                                                 HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries Value: MLMM:Systemicul Femicul Folia (1825-1835) 4847-00a0c91efb8b} ##7#storage#volume#{e29ac6c3-7037-11de-816d-806e6f6e6963}#0000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} [deviceinstance] Queries value: MLMM:System:Currentcontrolset/control/deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} ##7#storage#volume#{e29ac6c3-7037-11de-816d-806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} [deviceinstance]
                                                                 HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
```

```
806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLMN\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\f1c1ea40-e477-11e4-9632-
806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\f1c1ea40-e477-11e4-9632-
806e6f6e6963}#0000000000006500000#{5375630d-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\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot10#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                               HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot11#{53f5630d-b6bf-11d0-94f2-
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-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b\}\\ + *** torage**volumes napshot ** that diskvolumes napshot 4 ** (53f5630d-b6bf-11d0-94f2-00a0c91efb8b)[devicein stance]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\\ 53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\\##?\#storage\#volumesnapshot\#harddiskvolumesnapshot\#\\ 53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11c94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
9412-UU3UC91E1100J\mi:msco.usgan---
00a0291efb8b}[deviceinstance]
Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot8#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                               HKLM\system\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:
Queries value: "nt.mi\systemi\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-deries\delta\text{Substance}\]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-deries\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta\text{Substance}\delta
85bb-30ff1f953599}[default]
                                                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-30ffff953599){deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
                                              HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
  Oueries value:
Queries 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:
Queries value: m.t.m\system\currentcontrolset\current\currentcass\current\currentcass\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\
bcf7-00aa00b7b32a}[default]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
bcf7-00aa00b7b32a}\##?#acpi#pnp0c0a#0#{72631e54-78a4-11d0-bcf7-00aa00b7b32a}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
a537-0000f8753ed1}[default]
  Oueries value:
                                              HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
a537-0000f8753ed1}\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-
0000f8753ed1}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[default]
  Oueries value:
                                              HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}\##?#display#default_monitor#4&2abfaa30&0&12345678&00&02#{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\866519b5-3f07-4c97-b7df-24c5d8a8ccb8\\##?#display#default_monitor#582dcf5eab80812345678&06805#\\866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}\##?#display#default_monitor#5&2fab8e39&0&12345678&06&05#{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Queries value:
bc8c-00a0c91405dd\}[default]\\ Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-bc8c-00a0c91405dd}\*"?\#acpi\#pnp0303\#4&1d401fb5&0\#{884b96c3-56ef-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1-bc8c-11d1
00a0c91405dd}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Queries value:
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c
00a0c91405dd}[deviceinstance]
                                               HKLM\svstem\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Oueries value:
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&0000#{884b96c3-56ef-11d1-bc8c
00a0c91405dd}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\\ 884b96c3-56ef-11d1-bc8c-00a0c91405dd\\#?#root#rdp_kbd#0000#\\\\ 884b96c3-56ef-11d1-bc8c-00a0c91405dd\\\\ [deviceinstance]
   Oueries value:
                                               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]
  Oueries 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-
359c-8bef029dbdd0}\##?#acpi#genuineintel__x86_family_6_model_15__
_intel(r)_xeon(r)_cpu___x3220_@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-
_intel(r)_xeon(r)_cpu______
8bef029dbdd0}[deviceinstance]
  Oueries value
                                               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}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
8bef029dbdd0}[deviceinstance]
                                                 HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-
   Oueries value
```

```
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]
OUCU410971097[Juve12e115131ce]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#fac72212e15ea84#\a5dcbf10-6530-11d2-901f-
00c04fb951ed}[deviceinstance]
                                             HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}[default]
Oueries 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]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
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#{ad498944762f-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\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Queries value:
8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
   Oueries value:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
00c04fc3358c}[deviceinstance]
\label{lem:lem:queries} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc3358c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944-762f-11d0-8dcb-00c04fc356c}\width=\colored{ad498944
00c04fc3358c}[deviceinstance]
                                             HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
Oueries value: HKLM\system\currentcontrolset\control\deviceclas
8dcb-00c04fc3358c}\#?#root#ms_ndiswanipv6#0000#{ad498944-762f-11d0-8dcb-
                                             HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
00c04fc3358c}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Queries value:
8dcb-00c04fc3358c}\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
  Oueries value:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_pptpminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
Oueries value: HKLMsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#ms_sstpminiport#0000#{ad498944-762f-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]
                                             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]
  Queries value:
                                            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}[deviceinstance]
                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
   Oueries value:
Queries Value: httm://www.system.currentconfortset/sec114s2as34s34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2as34s2a
82e6-71a87abac361}\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}{deviceinstance}
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_agilevpnminiport#0000#{cac88484-7515-4c03-82e6-
7.1887abac361}{deviceinstance}
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_12tpminiport#0000#{cac88484-7515-4c03-82e6
71a87abac361}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Oueries value:
82e6-71a87abac361}\##?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
Queries value: HKLM/system\currentcontrolset\control\devicec!
82e6-71a87abac361}\##?#root#ms_ndiswanip#0000#{cac88484-7515-4c03-82e6-
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclas 82e6-71a87abac361}\##?#root#ms_ndiswanipv6#0000#{cac88484-7515-4c03-82e6-
                                             HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
71a87abac361}[deviceinstance]
                                             HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Queries value:
82e6-71a87abac361}\##?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Oueries value:
82e6-71a87abac361}\##?#root#ms_sstpminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
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]
                                             HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
ac88-96b894c191e2}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-ac88-96b894c191e2}\\##?\acpi\pnp0c0a\#0\#\{e849804e-c719-43d8-ac88-96b894c191e2}\\[deviceinstance]
                                             HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
  Oueries value:
bcaa-942b18988098}[default]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
  Oueries value:
bcaa-942b18988098}\##?#usb#root_hub#4&152cc752&0#{ed8cf6b1-62d5-4597-bcaa
942b18988098}[deviceinstance]
                                             HKLM\svstem\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
```

```
Oueries value:
                                   HKLM\svstem\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&22939226&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub#4824693ec3&0#\f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
                                   HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
  Oueries value:
                                  HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
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]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#vid_04b4&pid_6560#5&39c97729&083#\{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
                                   HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
                                   HKLM\software\microsoft\cryptography\oid\encodingtype
  Queries value:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7[name]
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
  Queries value
HKLM\system\currentcontrolset\enum\umb\1&841921d&0&printerbusenumerator[service]
  Oueries value:
HKLM\system\currentcontrolset\enum\umb\1&841921d&0&printerbusenumerator[classguid]
  Oueries value:
                                  HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
08002be10318}[lowerfilters]
  Queries value:
HKLM\system\currentcontrolset\enum\umb\umb\18841921d&0&printerbusenumerator[lowerfilters]
Queries value: HKLM\system\currentcontrolset\services\umbus\enum[count]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\services\umbus\enum[0]
                                   HKLM\system\currentcontrolset\services\umbus\enum[1]
  Oueries 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\enum\umb\1&841921d&0&printerbusenumerator[upperfilters]
                                   HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
08002be10318}[upperfilters]
                                   HKLM\software\microsoft\cryptography\oid\encodingtype
  Queries value
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
 Oueries value:
                                  HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7[name]
                                   HKLM\software\microsoft\cryptography\oid\encodingtype
  Oueries value:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7[name]
  Queries value:
\label{local-problem} HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio] \\ Queries\ value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize] \\
                                   HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
  Oueries value:
  Oueries value
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedllunloadonstop]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\compatibility32[spoolsv]
                                   HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion[devicepath]
HKLM\system\currentcontrolset\control\wmi\security[c9bf4a9e-d547-4d11-
  Queries value:
8242-e03a18h5he011
  Queries value:
                                    HKLM\system\currentcontrolset\control\print[exceptionhandlerenabled]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\print[threadnotifvmax]
  Queries value:
                                   HKLM\system\currentcontrolset\control\print[threadnotifyidlelife]
HKLM\system\currentcontrolset\control\print[threadnotifyidlelife]
  Queries value:
                                   HKLM\system\currentcontrolset\control\print[maxrpcsize]
HKLM\system\currentcontrolset\control\print[maxrpccalls]
  Oueries value
  Queries value:
  Oueries value:
                                   HKLM\software\microsoft\sqmclient\windows\disabledprocesses[71e8376c]
  Queries value:
                                    HKLM\system\currentcontrolset\control\print[callexitprocessonshutdox
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableipsourcerouting]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[arpretrycount]
  Queries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[igmplevel]
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[igmpversion]
  Queries value:
  Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableaddrmaskreply]
  Queries value:
\label{thm:local_hklm} \verb+KLM\system\currentcontrolset\services\tcpip\parameters[disabletaskoffload]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablebcastarpreply]
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledhcpmediasense]
  Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[disablemediasenseeventlog]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablemulticastforwarding]
  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[tcpuserfc1122urgentpointer]
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdataretransmissions]
  Queries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
  Queries value
\label{local-problem} HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval] Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcptimedwaitdelay]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpfinwait2delay]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtubhdetect]
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[tcp1323opts]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[enabletcpa]
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[enabledca]
  Queries value:
  Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[minimumpacketsizetodma]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableconnectionratelimiting]
```

```
Oueries value:
                                                                       HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
     Oueries value
HKLM \setminus System \setminus Current \subset Strong \setminus St
     Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationenabled]
     Oueries value:
Queries value:
\label{local-holes} \begin{split} &\text{HKLM} \xspstem \xspst
                                                                       HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
     Oueries value:
                                                                      HKLM\system\currentcontrolset\services\tcpip\parameters[arpuseethersnap]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[overridedefaultaddressselection]
    Oueries value:
                                                                      HKLM\system\currentcontrolset\services\tcpip\parameters[maxuserport]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[ipaddress]
     Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253\}[subnetmask]
     Oueries value:
c19ce8a73253}[ipautoconfigurationaddress]
     Oueries value
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[ipautoconfigurationenabled]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[performrouterdiscovery]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[defaultgateway]
     Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253\}[defaultgatewaymetric]
     Oueries value:
c19ce8a73253}[solicitationaddressbcast]
c19ce8a73253}[usezerobroadcast]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[typeofinterface]
Queries value:
c19ce8a73253}[mtu]
     Oueries value:
HKLMNsystem \current control set \services \tcpip\parameters \time faces \{128919e8-8a5e-41d1-ac17-c19c8a73253\} [interfacemetric]
     Oueries value
c19ce8a73253}[tcpackfrequency]
     Queries value:
c19ce8a73253}[tcpdelackticks]
                                                                      HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
     Oueries value:
\label{thm:local_hamman_hamman} \begin{tabular}{ll} HKLM \end{tabular} $HKLM \end{tabular} $$ is the local control set \end{tabular} $$ is the local contr
    Queries value:
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 100e&subsys 001e8086&rev 02\3&267a616a&0&18[driver]
                                                                       HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\linkage[upperbind]
     Queries value
                                                                      HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
     Queries value
Queries value: \text{MCLmSystem Correct Factors of the Correct Facto
     Oueries value:
                                                                       HKLM\software\microsoft\com3\finalizeractivitybypass1
     Queries value:
                                                                      HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid[]
HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
     Queries value:
                                                                      HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid[]
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}[]
     Oueries value
     Queries value:
                                                                       HKLM\system\currentcontrolset\services\vss\settings[idletimeout]
     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[]
     Oueries value:
                                                                       HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
      Queries value:
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid[]
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}[]
     Queries value:
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[inprocserver32]
                                                                      HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[1
     Oueries value:
                                                                       HKCR\clsid\{4e14fba2-2e22-11d1-9964-
      Queries value
00c04fbbb345}\inprocserver32[threadingmodel]
    Queries value:
Queries value:
                                                                      HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                                                       HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32[]
     Oueries value:
                                                                      HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[]
HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
     Queries value
     Oueries value:
00c04fb926af}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
     Oueries value:
                                                                       HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocse
                                                                     er32[threadingmodel]
                                                                       HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
     Oueries value:
                                                                      HKCR\interface\{00000100-0000-0000-0000-000000000046}\proxystubclsid32[] HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
     Queries value:
     Queries value:
     Oueries value:
                                                                       \label{localization} HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid[]
     Queries value:
                                                                        HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-
     Oueries value
0080c7d771bf}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
     Oueries value
                                                                       HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocser
                                                                    /er32[threadingmodel]
                                                                       HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
    Oueries value:
                                                                      HKCR\interface\{000000c-0000-0000-c000-00000000046}\proxystubclsid32[]
HKLM\software\microsoft\windows nt\currentversion\svchost[wersvcgroup]
     Queries value:
     Queries value:
     Oueries value
                                                                       HKLM\system\currentcontrolset\services\wersvc\parameters[servicedll]
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:
```

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

```
Oueries value:
                                                                HKLM\software\microsoft\windows nt\currentversion\svchost[imgsvc]
    Oueries value:
                                                                HKLM\system\currentcontrolset\services\stisvc\parameters[servicedll]
   Queries value:
\label{local-problem} HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest] \\ Queries\ value: HKLM\system\currentcontrolset\services\stisvc\parameters[servicemain] \\
   Oueries value:
\label{limage} \verb|HKLM| system| current controls et \controls tillimage \trace[suppress process output]| | The tillimage \controls tillimage \con
   Queries value:
                                                                HKLM\system\currentcontrolset\control\stillimage\trace[maxfilesize]
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\trace[defaulttraceflags]
   Oueries value:
                                                                HKLM\svstem\currentcontrolset\control\stillimage\trace[defaulttracemask]
    Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracelevel]
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\trace[defaultmaxtracearraysize]
   Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaultenableobjecttracking]

Queries value: HKLM\system\currentcontrol\set\control\stillimage\trace[heapoptions]
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[traceflags]
   Oueries value:
\label{thm:hammon} HKLMhsystem \current control still image \trace \wiaservc.dl1[tracemask] \\ Queries value:
\label{limited} HKLM \noindent \no
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dllfmaxtracearraysizel
    Queries 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]
                                                                \label{local-hkcR} HKCR\appid\alfaler26-8cfl-11d1-bf92-0060081ed811\ [authenticationlevel] \\ HKCR\appid\alfaler26-8cfl-11d1-bf92-0060081ed811\ [accesspermission] \\
     Queries value:
   Queries value:
   Queries value:
Queries value:
                                                                HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\progid[]
HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[]
                                                                HKLM\software\microsoft\sqmclient\windows\disabledprocesses[34dba8a7]
HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}[]
HKLM\system\currentcontrolset\control\stillimage[deviceid]
   Oueries value:
     Queries value:
    Queries value:
    Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected[defaulthandler]
                                                                HKLM\system\currentcontrolset\control\stillimage\events\connected[guid]
   Oueries value:
     Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\f38f8a702-36bb-4a68-80e6
d4966b9bb718}[name]
   Queries value:
d4966b9bb718}[desc]
   Oueries value:
HKLMNsystem \current control still image \events \connected \ \{38f8a702-36bb-4a68-80e6-d4966b9b718\} [icon]
   Oueries value
d4966b9bb718}[cmdline]
   Queries value
Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[guid]
   Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage[defaulthandler]

Queries value: HKLM\system\currentcontrolset\control\stillimage\events\emailimage[guid]
    Oueries value:
759eb35cdf9a}[name1
    Queries value
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc1
    Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
   Queries value:
\label{limage} HKLM\system\currentcontrolset\control\stillimage\events\emailimage\diage\diage\final for the control of the c
   Oueries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage[defaulthandler]

Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage[guid]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[name1
    Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc]
   Queries value:
Queries value:
\label{limage-events-faximage-faximage-events-faximage-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faximage-events-faxim
   Oueries value:
HKLM\svstem\currentcontrolset\control\stillimage\events\printimage[guid]
   Oueries value:
    Queries value:
759eb35cdf9a}[name1
    Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc]
   Queries value:
\label{limage-events-printimage-decomposition} HKLM\system\control\stillimage-events-printimage-diagrams (d13e3f25-1688-45a0-9743-759eb35cdf9a)[icon]
   Oueries value
HKLMNsystem \current control set \control still image \events \print image \d13e3f25-1688-45a0-9743-759eb35cdf9a\color=[cmdline]
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[defaulthandler]
   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]
   Queries value:
d4966b9bb718}[desc]
   Queries value:
\label{limage} HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-d4966b9b718\}[icon]}
    Oueries value
```

```
d4966b9bb718}[cmdline]
    Queries value
783ce7a92f22}[name1
    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]
   Oueries value
783ce7a92f22}[cmdline]
   Oueries value
759eb35cdf9a}[name1
    Queries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc1
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
   Queries value:
\label{limage} HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
   Oueries value:
HKLMNsystem \current control set \control \still image \events \scan but ton \eabbd 70d-a25f-4e90-96a4-7105fd3b53b1 \[ name \] \\
   Queries value:
\label{thm:control} HKLM \system \control still image \events \scan button \eabbd 70d-a 25f-4e 90-96a 4-4e 90-96
7105fd3b53b1}[desc1
     Queries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}[icon]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}[cmdline]
   Queries value:
\label{thm:local_hamma} \begin{tabular}{llll} HKLM \end{tabular} is the local control still image \end{tabular} events \end{tabular} is the local control still image \end{tabular} events \end{tabular} is the local control still image \end{tabular} events \end{tabular} events \end{tabular} is the local control still image \end{tabular} events \end{tabular} events
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[guid]
HKLM\system\currentcontrolset\control\stillimage\serversettings[shutdownifunuseddelav]
   Queries value:
Queries value:
                                                             HKLM\system\currentcontrolset\services\nativewifip[imagepath]
HKLM\system\currentcontrolset\services\nativewifip[objectname]
   Oueries value:
                                                              HKLM\system\currentcontrolset\services\nativewifip[type]
    Queries value:
                                                               HKLM\system\currentcontrolset\services\nativewifip\enum[count]
   Oueries value:
                                                              HKLM\system\currentcontrolset\services\nativewifip[displayname]
    Queries value:
                                                              \label{local_ham} \verb+KLM\system\currentcontrolset\enum\root\legacy\_native wifip\0000[service]
   Queries value:
\label{local-problem} HKLM \noindent The MKLM \no
0000f8753ed1}[lowerfilters]
    Queries value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[lowerfilters]
   Oueries value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[upperfilters]
                                                             HKLM\svstem\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-
   Oueries value:
0000f8753ed1}[upperfilters]
                                                              HKLM\system\currentcontrolset\services\nativewifip[pnpflags]
   Queries value:
   Oueries value
                                                              HKLM\svstem\currentcontrolset\control\wmi\securitv[d905ac1c-65e7-4242-
99ea-fe66a8355df8]
                                                              HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Oueries value
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1\\ndi[filtertype]
Queries value: HKLM\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:
                                                              Queries value
                                                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage[upperbind]
    Queries value:
                                                             HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
HKLM\system\currentcontrolset\services\ndisuio[imagepath]
   Queries value:
                                                             HKLM\system\currentcontrolset\services\ndisuio[objectname] HKLM\system\currentcontrolset\services\ndisuio[type]
    Oueries value:
    Queries value:
   Oueries value:
                                                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\link
                                                            ge[upperbind]
                                                              HKLM\system\currentcontrolset\services\ndisuio\enum[count]
   Queries value:
                                                             HKLM\system\currentcontrolset\services\ndisuio[displayname]
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
    Oueries value:
    Queries value:
    Oueries value:
                                                              HKLM \verb|\system| current controls et \verb|\enum| root \verb|\legacy_ndisuio| 0000[class guid]|
     Queries value
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[lowerfilters]
    Oueries value:
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[upperfilters]
   Oueries value:
                                                              HKLM\system\currentcontrolset\services\ndisuio[pnpflags]
Queries value:
aded-5304bf8f636d]
                                                              HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-
Queries value:
adfc-50f1888138ab]
                                                              HKLM\system\currentcontrolset\control\wmi\security[b3eee223-d0a9-40cd-
   Oueries value:
                                                              HKLM\svstem\currentcontrolset\enum\root\ms sstpminiport\0000[driver]
                                                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[upperbind]
                                                             HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value
   Queries value
08002be10318\} \\ 0003 \\ \label{eq:controlset} \\ 08002be10318\} \\ 0903 \\ \label{eq:controlset} \\ 09003 \\ \label{eq:controlset} \\ \label{eq:controlset} \\ \label{eq:controlset} \\ 09002be10318\} \\ \label{eq:controlset} \\ 09003 \\ \label{eq:controlset} \\ \label{eq:controlset} \\ 09002be10318\} \\ \label{eq:controlset} \\ 09003 \\ \label{eq:controlset} \\ 09003 \\ \label{eq:controlset} \\ 09002be10318\} \\ \label{eq:controlset} \\ 09003 \\ \label{eq:controlset} \\ 09003 \\ \label{eq:controlset} \\ 09002be10318\} \\ \label{eq:controlset} \\ 09003 \\ \label{eq:cont
   Oueries value
                                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage[upperbind]
                                                              HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000[driver]
   Queries value:
Oueries value:
                                                              HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
Queries value: HKLM\system\
08002be10318}\0001\linkage[upperbind]
                                                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value
                                                              HKLM\svstem\currentcontrolset\enum\root\*teredo\0000[driver
                                                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage[upperbind]
                                                             HKLM\system\currentcontrolset\enum\root\*isatap\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value:
   Queries value
08002be10318}\0009\linkage[upperbind]
    Queries value:
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
```

HKLM\system\currentcontrolset\control\wmi\autologger\circular

Queries value

```
context logger[start]
   Queries value
                                            {\tt HKLM \control \c
context logger[flushthreshold]
  Oueries value
                                           HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[buf
  Oueries value
                                            HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[minim
                                     mbuffers1
                                            HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Queries value
context logger[flushtimer]
Queries value: H
                                            HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maximumbuffers]
                                           HKLM\system\c
   Queries value
                                                                    urrentcontrolset\control\wmi\autologger\circular kernel
context logger[filename]
  Oueries value
                                           HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[enablekernelflags]
  Oueries value
                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[s
                                     alkingfilter]
                                            HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Queries value
context logger[clo
Queries value:
                                            ,
HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maxfilesize]
   Queries value
                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[logfilemode]
  Oueries value
                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[disable
                                         ealtimepersistence]
  Oueries value
                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[guid]
                                            HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
  Queries value
context logger[filecounter]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filemax]
                                            {\tt HKLM \control \c
context logger[pooltagfilter]
Queries value:
af71-3e63d056f174]
                                            HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-
  Oueries value:
                                            HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac[configflags]
                                            HKLM\system\currentcontrolset\enum\root\system\0000[hardwareid]
   Queries value
   Queries value
                                           \label{local-hklm-system-control} HKLM\system\currentcontrolset\enum\root\system\0000[compatibleids]\\ HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-}
   Queries value
00805fc1270e}\asvncmac\control[disablecount]
                                            HKLM \setminus system \setminus current controlset \setminus enum \setminus sw \setminus \{eeab7790-c514-11d1-b42b\}
00805fc1270e}\asyn
                                  mac[service]
   Oueries value
                                           HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asy
                                    ac[classguid]
  Oueries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}[lov
                                           HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
  Oueries value
00805fc1270e}\asyn
                                  mac[lowerfilters]

HKLM\system\currentcontrolset\services\asyncmac\enum[count]
  Queries value
   Oueries value
                                            HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac[upperfilters]
  Oueries value
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}[upperfilters]
                                            HKLM\system\currentcontrolset\services\asyncmac[objectname]
   Queries value
                                            HKLM\system\currentcontrolset\services\asyncmac[type]
   Oueries value
   Queries value:
                                            HKLM\system\currentcontrolset\services\asyncmac[star
   Oueries value:
                                            HKLM\svstem\currentcontrolset\services\asvncmac[bootflags]
   Queries value:
                                           HKLM\system\currentcontrolset\services\asyncmac[imagepath]
HKLM\system\currentcontrolset\services\asyncmac\enum[0]
   Queries value
                                            HKLM\system\currentcontrolset\services\asyncmac[pnpflags
   Oueries value
                                            HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b
00805fc1270e}\asvncmac[driver]
   Queries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010\linkage[export]
   Oueries valu
                                            HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1
08002be10318}\0010[characteristics]
  Oueries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Queries value. MKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                  *physicalmediatype]
HKLM\system\cur
08002be10318}\0010I
   Queries value
08002be10318}\0010[netcfginstanceid]
                                            HKLM\system\c
08002be10318}\0010[*iftype]
   Oueries value
                                            HKI M\system\currentcontrolset\control\class\{4d36e972-e325-11ce-hfc1-
08002be10318}\0010[netluidindex]
  Oueries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                  filterclass]
08002be10318}\0010
                                            HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
  Queries value
00805fc1270e}\
                                       [friendlyname]
                                            HKLM\system\cur
   Queries value
00805fc1270e}\as
                                    ac[devicedesc]
                                            HKLM\system
   Queries value
00805fc1270e}\asyı
                                   mac[uinumber]
Queries value: HKLM\system\ci
08002be10318}\0010\linkage[rootdevice]
                                                                         entcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Oueries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010\link
                                         age[filterlist]
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1
  Oueries value
HKLM\system\cur
08002be10318}\0010[slotnumber1
Queries value: HKLM\syst: 08002be10318}\0010[remotebootcard]
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Oueries value
                                           HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\001
                                          disconnecttosleeptimeout]
  Oueries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
                                           onpattern]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value
08002he103183\0010
                                           onmagicpacket1
   Queries value
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
                                   devicesleepondisconnect1
Queries value: HKLM\sys
08002be10318}\0010[*pmarpoffload]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Oueries value
                                           HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[
                                          offload]
  Oueries value
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[
                                         vifirekeyoffload]
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
08002be10318}\0010[sgma
                                          registersneeded]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Queries value
08002be10318}\0010[ndisdriververifvflags]
                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
```

```
08002be10318}\0010[*ipchecksumoffloadipv4]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries valu
08002be10318}\0010[*tcpchecksumoffloadipv4]
 Oueries value
                          HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
                          necksumoffloadipv4]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[*tcpchecksumoffloadipv6]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\0010[*udpchecksumoffloadipv61
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
                         udpchecksumoffloadipv41
Queries value:
08002be10318}\0010[
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                     tcpudpchecksumoffloadipv6]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[
                         2ipv6]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[*lsov2ipv4]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002he10318}\0010[*lsov1inv4]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\0010
                     ipsecoffloadv1ipv41
                     HKLM\system\currentcontrol\set\control\class\\{4d36e972-e325-11ce-bfc1-\text{tcpconnectionoffloadipv4}}
Queries value:
08002be10318}\0010[
                         Queries value
08002be10318}\0010[
 Oueries value
                          HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                         coffloadv2]
08002be10318}\0010
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\0010[*ipsecoffloadv2ipv4]

Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
                     numanodeid1
Queries value:
08002be10318}\0010[
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                     *maxrssprocessors]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[
                         aseprocgroup]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010
 Queries value
                          HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\as
Queries value:
                         devicetype]

HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\pi
                     ties[devicetype]
                           HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b
00805fc1270e}\asy
                     ac[exclusive]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\pr
                      ties[exclusive]
 Oueries value
                          HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asy
                      ac[devicecharacteristics]
                          HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value
08002be10318}\pro
                      ies[devicecharacteristics]
                          HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
 Queries value
00805fc1270e}\a
                       cſsecuritvl
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\pro
                      ties[security]
Queries value:
00805fc1270e}\asy
                          HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
                        logconf[forcedconfig]
 Oueries value
                          HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asy
                        logconf[overrideconfigvector]
 Oueries value
                          HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asy
                          ogconf[bootconfig]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\0010\linkage[upperbind]

Queries value: HKLM\system\currentcontrolset\services\ndiswan[ndisbootstart]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[irps
                         acksize1
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\0010[maxframesize]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
08002be10318}\0010[framesperport]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries valu
08002be10318}\0010[xonxoff]
 Oueries value
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[time
                        outbase]
 Oueries value
                          HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[tim
                          utbaud]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value
                         outresync]

HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[tim
 Queries value
08002be10318}\0010[writebufferingenabled]
                          HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[extendedxonxoffenabled]
\label{thm:local_Queries} Queries value: $$HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010[portauthsendcontrolstate]
 Oueries value
                          HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[*ndisdevicetype]
                          HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 Queries value
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}\#\control[linked]
82e6-71a87abac361}\control[referencecount]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-
8dcb-00c04fc3358c}\#{e2f8a220-af88-446c-9a55-453e58dd3a33}\control[linked]
Queries value: HKLM\system\currentcontrolset\control\deviceclasse\\ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-
8dcb-00c04fc3358c}\control[referencecount]
 Sets/Creates value
                          HKLM\system\currentcontrolset\enum\root\legacy_nativewifip[nextinstance]
 Sets/Creates value
HKLM\system\currentcont
                         olset\enum\root\legacy_nativewifip\0000\control[*newlycreated*]
 Sets/Creates value
                          HKLM\system\currentcontrolset\enum\root\legacy nativewifip\0000[service]
 Sets/Creates value
                          HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[legacy]
 Sets/Creates value
Sets/Creates value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[classguid]
 Sets/Creates value
\label{local-holes} HKLM\system\currentcontrolset\enum\root\legacy\_native\wifip\0000[devicedesc] \\ Sets/Creates\value: HKLM\system\currentcontrolset\services\native\wifip\enum[0] \\
 Sets/Creates value
                          HKLM\system\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]
                           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*1
     Sets/Creates value:
                                                                 HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
     Sets/Creates value:
                                                                HKLM\system\currentcontrolset\enum\root\legacv ndisuio\0000[legacv]
                                                                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]
     Sets/Creates value
                                                                 HKLM\system\currentcontrolset\services\ndisuio[ndisminorversion]
     Sets/Creates value
                                                                 HKLM\system\currentcontrolset\services\asyncmac\enum[0]
                                                                HKLM\system\currentcontrolset\services\asyncmac\enum[count]
HKLM\system\currentcontrolset\services\asyncmac\enum[nextinstance]
     Sets/Creates value
     Sets/Creates value
    Sets/Creates value
                                                                HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac\
                                                               ontrol[activeservice]
                                                                HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
    Sets/Creates value
82e6-71a87abac361\} \\ \text{##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}} \\ \text{#asyncmac#{cac88484-7515-4c03-b42b-00805fc1270e}} \\ \text{#asyncmac#{cac88484-7515-4
82e6-71a87abac361}\#\control[linked]
   Sets/Creates value:
                                                              HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}\control[referencecount]
Sets/Creates\ value: HKLMNsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\with a sweeper and the sets of the s
8dcb-00c04fc3358c}\#{e2f8a220-af88-446c-9a55-453e58dd3a33}\control[linked]
Sets/Creates value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-
8dcb-00c04fc3358c}\control[referencecount]

Value changes: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e
32c86e1ba19f}\#\control[linked]
                                                              HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
    Value changes:
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-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1843e-1844e-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-1844
32c86e1ba19f}\control[referencecount]
                                                                HKLM\svstem\currentcontrolset\services\umbus\enum[count]
    Value changes:
                                                                 HKLM\system\currentcontrolset\services\umbus\enum[nextinstance]
     Value changes:
     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\svstem\currentcontrolset\services\ndisuio\enum[nextinstance]
     Value changes
                                                                 HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[status]
Value changes: HKLM\system 00805fc1270e}\asyncmac[capabilities]
                                                                Value change
                                                                HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
00805fc1270e}\asyncmac[uinumber]
                                                                HKLM\svstem\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
    Value changes
00805fc1270e}\asyncmac[hardwareid]
                                                                HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
    Value changes:
00805fc1270e}\asvncmac[containerid]
                                                                HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
     Value changes:
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03
82e6-71a87abac361}[deviceinstance]
                                                              HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
   Value changes:
82e6-71a87abac361}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03
82e6-71a87abac361}\#[symboliclink]
   Value changes:
                                                              HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}[deviceinstance]
Value changes: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}\#{e2f8a220-af88-446c-9a55-453e58dd3a33}[symboliclink]
```