Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID: Risk Level:

Date Processed: 2016-04-08 09:39:51 (UTC)

61.4 seconds IntelliVM Processing Time Virtual Environment:

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

Sample ID Type: basic Owner: admir

ToggleService32.exe Label Date Added: 2016-04-08 09:39:50 (UTC)

File Type: PE32:win32 File Size: 10254 bytes

MD5 1439e0552127dda0c66b7be1eadb723d

SHA256: 89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a

Description:

Pattern Matching Results

Modifies registry autorun entrie Writes to system32 folder

3 Program causes a crash [Info]
5 Installs service

PE: File has TLS callbacks

PE: Nonstandard section

3 Writes to a log file [Info]

4 Terminates process under Windows subfolder
4 Connects to local IP

3 Long sleep detected 2 Resolves local hostname

Static Events

Anomaly Contains a virtual section

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

Process/Thread Events

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

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

LocalServicePeerNet]

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

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

imgsvc]

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

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

Loads service: Loads service:

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

Loads service: Loads service: PNRPSvc [C:\Windows\System32\svchost.exe -k LocalServicePeerNet]
Spooler [C:\Windows\System32\spoolsv.exe]

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

Loads service: SysM LocalSystemNetworkRestricted]

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

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

LocalServiceNetworkRestr ricted]

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

LocalServiceNetworkRestricted1

Loads service: Loads service:

icted]
WERSVc [C:\Windows\System32\svchost.exe -k WerSvcGroup]
MpsSvc [C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork]
STISvc [C:\Windows\system32\svchost.exe -k imgsvc]
W32Time [C:\Windows\system32\svchost.exe -k LocalService]
WAUSErv [C:\Windows\system32\svchost.exe -k netsvcs]
WLANSvc [C:\Windows\system32\svchost.exe -k
rted! Loads service: Loads service: Loads service: Loads service:

LocalSystemNetworkRestricted]

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

Creates remote thread

Named Object Events

Creates mutex \Sessions\1\BaseNamedObjects\DBWinMutex \BaseNamedObjects\MSDTC_STATS_EVENT \BaseNamedObjects\{86B8BF1C-6469-4A5A-8707-540234EE8334}_S-1-5-19

Creates mutex

\BaseNamedObjects\WIATRACE_MUTEX
\BaseNamedObjects\ConsoleEvent-0x0000089C Creates mutex Creates event \BaseNamedObjects\SvcctrlStartEvent_A3752DX \KernelObjects\MaximumCommitCondition Creates event Creates event: Creates event: \BaseNamedObjects\TermSrvReadvEvent \BaseNamedUbjects\\ermSrvkeadyEvent
\Security\LSA_AUTHENTICATION_INITIALIZED
\BaseNamedObjects\RouterPreInitEvent
\KernelObjects\SystemErrorPortReady
\...\WerSvefystemPermissionsEvent
\BaseNamedObjects\WiaServiceStarted Creates event: Creates event Creates event:

File System Events

Creates event:

C:\Windows\System32\output.txt
C:\Windows\System32\Msdtc\Trace\dtctrace.log Creates

Creates Creates C:\Windows\ServiceProfiles\LocalService

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

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

```
Creates
                                  C:\ProgramData
  Creates:
                                  C:\ProgramData\Microsoft
                                  C:\ProgramData\Microsoft\Crypto
  Creates:
                                  C:\ProgramData\Microsoft\Crypto\RSA
C:\ProgramData\Microsoft\Crypto\RSA\
  Creates:
  Creates
  Creates:
                                  C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Creates:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\a15b793d2c05e5b7b6c03b4db2035d82_577c175f-2428-
49fc-a95e-635c93546ef9
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
                                  C:\Windows\Debug\WIA
C:\Windows\Prefetch\TOGGLESERVICE32.EXE-2248A864.pf
 Creates:
  Opens:
  Opens:
                                  C:\Windows\Svstem32
                                  C:\Windows\System32\sechost.dll
C:\Windows\System32\output.txt
  Opens:
  Opens:
  Opens:
                                  C:\Windows\Prefetch\ALG.EXE-1D11534C.pf
                                  C:\Windows\System32\atl.dll
  Opens:
  Opens:
                                  C:\Windows\Svstem32\wsock32.dll
                                  C:\Windows\System32\mswsock.dl1
C:\Windows\System32\imm32.dl1
  Opens:
  Opens:
Opens:
                                  C:\Windows\System32\en-US\alg.exe.mui
C:\Windows\System32\rpcss.dll
                                  C:\Windows\System32\cryptbase.dll
C:\Windows\System32\cryptsp.dll
C:\Windows\System32\rsaenh.dll
  Opens:
  Opens:
  Opens:
Opens:
                                  C:\Windows\Globalization\Sorting\SortDefault.nls
C:\Windows\System32\RpcRtRemote.dl1
  Opens:
                                  C:\Windows\Prefetch\MSDTC.EXE-CC1DEC77.pf
                                  C:\Windows\System32\msdtctm.dll
C:\Windows\System32\msdtcprx.dll
  Opens:
                                  C:\Windows\System32\mtxclu.dll
C:\Windows\System32\clusapi.dll
  Opens:
  Opens:
                                  C:\Windows\System32\cryptdll.dll
C:\Windows\System32\resutils.dll
C:\Windows\System32\version.dll
  Opens:
  Opens:
  Opens:
  Opens:
                                  C:\Windows\System32\bcrypt.dll
C:\Windows\System32\ktmw32.dll
  Opens:
  Opens:
                                  C:\Windows\System32\msdtclog.dll
                                  C:\Windows\System32\winmm.dll
C:\Windows\System32\xolehlp.dll
  Opens:
  Opens:
  Opens:
                                  C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\msdtc.exe.mui
  Opens:
  Opens:
                                  C:\Windows\System32\comres.dll
                                  C:\Windows\System32\msdtcVSp1res.dll
C:\Windows\System32\mtxoci.dll
  Opens:
  Opens:
  Opens:
                                  C:\Windows\System32\oci.dll
C:\Windows\system32\oci.dll
  Opens:
                                  C:\Windows\system\oci.dll
C:\Windows\oci.dll
  Opens:
  Opens:
                                  C:\Windows\Svstem32\Wbem\oci.dll
  Opens:
  Opens:
                                  C:\Windows\System32\WindowsPowerShell\v1.0\oci.dll
C:\Windows\System32\Msdtc\Trace
  Opens:
  Opens
                                  C:\Windows\Prefetch\UIIODETECT_EXE-A794C8BB_nf
                                  C:\Windows\System32\wtsapi32.dll
  Opens:
  Opens:
                                  C:\Windows\Svstem32\winsta.dll
  Opens:
                                  C:\Windows\system32\MSDtc\trace\dtctrace.log
C:\Windows\System32\en-US\ui0detect.exe.mui
  Opens:
                                  C:\Windows\System32\W1S0WndH.d11
C:\Windows\System32\ole32.d11
  Opens
  Opens

        Opens:
        C:\Windows\system32\UIODetect.exe.Local\

        Opens:
        C:\Windows\winxxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

                                  C:\Windows\winsxs\x86 microsoft.windows.comr
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens:
                                  C:\Windows\WindowsShell.Manifest
                                  C:\Windows\System32\duser.dll
C:\Windows\System32\uxtheme.dll
  Opens:
  Opens:
                                  C:\Windows\System32\dwmapi.dll
C:\Windows\System32\xmllite.dll
  Opens:
  Opens:

        Opens:
        C:\Windows\System32\en-U5\duser.dl1.mui

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

        controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9

\label{lem:opens:controls} Opens: C: \windows \winsxs \x86\_microsoft.windows.c..- controls.resources\_6595b64144ccf1df\_6.0.7600.16385\_en-us\_581cd2bf5825dde9 \comctl32.dll.mui
 Opens:
                                  C:\Windows\Svstem32\imageres.dll
                                  C:\Windows\System32\en-US\imageres.dll.mui
C:\Windows\Fonts\StaticCache.dat
  Opens:
  Opens:
  Opens:
                                  C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
  Opens:
                                  C:\$Extend
  Opens:
                                  C:\ProgramData
C:\ProgramData\Microsoft
  Opens:
  Opens:
  Opens:
                                  C:\ProgramData\Microsoft\Crypto
C:\ProgramData\Microsoft\Crypto\RSA
  Opens:
  Opens:
                                  C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
  Opens:
                                  C:\Windows\Globalization
  Opens:
                                  C:\Windows\Globalization\Sorting
C:\Windows\Microsoft.NET
  Opens:
  Opens:
  Opens:
                                  C:\Windows\ServiceProfiles
                                  C:\Windows\ServiceProfiles\LocalService
  Opens:
  Opens:
                                  C:\Windows\ServiceProfiles\LocalService\AppData
                                  C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
  Opens:
  Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c
  Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\f8d4f95592ce335421d51fadb8712f5c\grouping
Opens: C:\Windows\System32\DriverStore
                                  C:\Windows\System32\DriverStore\en-US
 Opens:
                                  C:\Windows\System32\en-US
C:\Windows\System32\ntdll.dll
  Opens:
  Opens:
                                  C:\Windows\System32\kernel32.dll
C:\Windows\System32\apisetschema.dll
  Opens
  Opens:
                                  C:\Windows\Svstem32\KernelBase.dll
  Opens:
                                  C:\Windows\System32\locale.nls
C:\Windows\System32\svchost.exe
  Opens:
  Opens:
                                  C:\Windows\System32\msvcrt.dll
C:\Windows\System32\rpcrt4.dll
  Opens:
  Opens:
  Opens:
                                  C:\Windows\Svstem32\DriverStore\en-US\ndiscap.inf loc
                                  C:\Windows\System32\userenv.dll
```

```
Opens:
                                                                    C:\Windows\Svstem32\profapi.dll
                                                                   C:\Windows\System32\gpapi.dl1
C:\Windows\System32\secur32.dl1
    Opens:
    Opens:
                                                                   C:\Windows\System32\sspicli.dll
C:\Windows\System32\credssp.dll
    Opens:
    Opens:
    Opens:
                                                                    C:\Windows\Svstem32\advapi32.dll
                                                                   C:\Windows\System32\shell32.dl1
C:\Windows\System32\shlwapi.dl1
    Opens:
    Opens:
                                                                   C:\Windows\System32\gdi32.dl1
C:\Windows\System32\user32.dl1
    Opens
    Opens:
    Opens:
                                                                    C:\Windows\Svstem32\lpk.dll
                                                                   C:\Windows\System32\usp10.dl1
C:\Windows\System32\msctf.dl1
    Opens:
    Opens:
                                                                   C:\Windows\System32\en-US\svchost.exe.mui
C:\Windows\System32\pnrpsvc.dl1
    Opens
    Opens:
                                                                   C:\Windows\System32\crypt32.dll
C:\Windows\System32\msasn1.dll
C:\Windows\System32\en-US\crypt32.dll.mui
    Opens:
    Opens:
    Opens:
    Opens:
                                                                    C:\WINDOWS\MICROSOFT.NET\NGENSERVICE_PRI1_LOCK.DAT
    Opens:
                                                                         :\Windows\System32\ncrypt.dll
                                                                   C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\en-US\p2pcollab.dll.mui
C:\Windows\System32\QAGENTRT.DLL
    Opens:
    Opens:
    Opens:
Opens:
                                                                   C:\Windows\System32\DriverStore\en-US\netrast.inf_loc
C:\Windows\System32\en-US\dnsapi.dll.mui
    Opens:
                                                                    C:\Windows\Svstem32\fveui.dll
                                                                    C:\Windows\System32\en-US\fveui.dll.mui
    Opens:
\verb|C:\widetilde{W}| indows \\ Service \\ Profiles \\ Local Service \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ idstore.sst.new \\ App Data \\ Roaming \\ Peer Networking \\ App Data \\ Roaming \\
    Opens
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
                                                                   C:\Windows\System32\ws2_32.dl1
C:\Windows\System32\nsi.dl1
    Opens:
    Opens:
                                                                   C:\Windows\System32\wship6.dll
C:\Windows\System32\IPHLPAPI.DLL
    Opens:
    Opens:
    Opens:
                                                                    C:\Windows\Svstem32\winnsi.dll
                                                                   C:\Windows\System32\dhcpcsvc6.dll
C:\Windows\System32\dhcpcsvc.dll
     Opens:
    Opens:
    Opens:
                                                                   C:\Windows\System32\sqmapi.dll
C:\Windows\System32\ssdpapi.dll
    Opens:
    Opens:
 C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f6af2fef0fc5f4f2bc6f75c1ff7fd887_577c175f-2428-
49fc-a95e-635c93546ef9
    Opens:
                                                                    C:\Windows\DtcInstall.log
                                                                    C:\Windows\System32\ntmarta.dll
    Opens:
    Opens:
                                                                    C:\Windows\System32\p2psvc.dll
                                                                    C:\Windows\System32\P2PGraph.dll
    Opens:
                                                                    C:\Windows\Svstem32\esent.dll
    Opens:
    Opens:
                                                                   C:\Windows\System32\slc.dll
C:\Windows\System32\psapi.dll
    Opens:
    Opens:
                                                                    C:\Windows\Svstem32\oleaut32.dll
                                                                    C:\Windows\System32\DriverStore\en-US\nettcpip.inf_loc
    Opens:
    Opens:
                                                                    C:\Windows\System32\authz.dll
    Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\6bd89088524e6a41cf86084fbbab0cc6_577c175f-2428-
49fc-a95e-635c93546ef9
    Opens:
                                                                    C:\Windows\System32\DriverStore\en-US\lltdio.inf_loc
    Opens:
C:\PROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\F0D041F93C731ACAA036AC2BD71BC124_577C175F-2428-
49FC-A95E-635C93546EF9
   Onens
                                                                    {\tt C:\Windows\System32\DriverStore\en-US\netsstpt.inf\_loc}\\
                                                                   C:\Windows\System32\pripnsp.dll
C:\Windows\System32\rasadhlp.dll
    Opens:
    Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\eb3bc6388b8f46d91ac65574d706a290_577c175f-2428-
49fc-a95e-635c93546ef9
C: \windows \ensuremath{\mbox{\mbox{$C$}}\xspace} \ensuremath{\mbox{$V$}\xspace} \ensuremat
C:\windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\8d844364c535c5b5c8ba03cedd538a73.sst
                                                                   C:\Windows\System32\Wldap32.dll
C:\Windows\System32\schannel.dll
    Opens:
    Opens
    Opens:
                                                                   C:\Windows\System32\DriverStore\en-US\netserv.inf_loc
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
   Opens:
                                                                    C:\Windows\Svstem32\Msdtc
                                                                   C:\Windows\System32\Msdtc\MSDTC.LOG
C:\Windows\System32\en-US\msdtcVSp1res.dll.mui
    Opens:
                                                                   C:\Windows\System32\FirewallAPI.dll
C:\Windows\Temp
    Opens:
    Opens:
    Opens:
                                                                    C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\a15b793d2c05e5b7b6c03b4db2035d82_577c175f-2428-
49fc-a95e-635c93546ef9
    Opens:
                                                                    C:\Windows\System32\en-US\QAgentRT.dll.mui
    Opens:
{\tt C: Windows Service Profiles \ Local Service \ App Data \ Roaming \ Peer Networking \ d636 cab 8b 49 d4d595 ad 3f 861 a 80 c057e.sst and the service \ Peer \ Normalization \ Peer \ Peer \ Normalization 
                                                                   C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
   Opens:
                                                                   C:\Windows\System32\powrprof.dll
C:\Windows\System32\en-US\spoolsv.exe.mui
    Opens:
    Opens:
                                                                   C:\Windows\System32\en-US\setupapi.dll.mui
C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
    Opens:
    Opens:
    Opens:
                                                                    C:\Windows\Svstem32\drivers\etc\lmhosts
                                                                   C:\Program Files
C:\Program Files\DVD Maker
    Opens:
    Opens:
                                                                    C:\Program Files\DVD Maker\Shared
    Opens:
    Opens:
                                                                    C:\Program Files\DVD Maker\Shared\DvdStyles
    Opens:
                                                                    C:\Users
                                                                   C:\Users\Admin
C:\Users\Admin\AppData
    Opens:
    Opens:
                                                                   C:\Users\Admin\AppData\Local
C:\Users\Admin\AppData\Local\Microsoft
    Opens
    Opens:
    Opens:
                                                                    C:\Users\Admin\AppData\Local\Microsoft\Windows
                                                                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Opens:
    Opens
Files\Content TE5
                                                                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
    Opens
Files\Content.IE5\KO5TVCON
                                                                   un
C:\Users\Admin\AppData\Roaming
C:\Users\Admin\AppData\Roaming\Microsoft
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My
    Opens:
    Opens:
    Opens:
    Opens:
                                                                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
```

```
Opens:
                                 C:\Windows\IME
                                 C:\Windows\IME\IMEJP10
  Opens:
                                 C:\Windows\Microsoft.NET\Framework
C:\Windows\Microsoft.NET\Framework\v2.0.50727
  Opens:
  Opens:
  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\catroot2
                                 C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}
C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
  Opens:
  Opens:
                                 C:\Windows\System32\com
C:\Windows\System32\SMI
  Opens:
  Opens:
  Opens:
                                 C:\Windows\Svstem32\SMI\Store
                                 C:\Windows\System32\rasctrs.dl1
C:\Windows\System32\VSSVC.exe
  Opens:
  Opens:
                                 C:\Windows\System32\vssapi.dll
C:\Windows\System32\vsstrace.dll
  Opens:
  Opens:
  Opens:
                                 C:\Windows\Svstem32\netapi32.dll
                                 C:\Windows\System32\netutils.dll
C:\Windows\System32\srvcli.dll
  Opens:
  Opens:
                                 C:\Windows\System32\wkscli.dll
C:\Windows\System32\samcli.dll
  Opens:
                                 C:\Windows\Svstem32\setupapi.dll
                                 C:\Windows\System32\cfgmgr32.dll
C:\Windows\System32\devobj.dll
  Opens:
  Opens:
Opens:
                                 C:\Windows\System32\virtdisk.dll
C:\Windows\System32\fltLib.dll
  Opens:
                                 C:\Windows\Svstem32\en-US\VSSVC.exe.mui
                                 C:\Windows\System32\clbcatq.dll
C:\Windows\System32\vss_ps.dll
  Opens:
                                 C:\Windows\System32\en-US\vsstrace.dll.mui
C:\Windows\System32\samlib.dll
  Opens:
  Opens:
  Opens:
                                 C:\Windows\Svstem32\es.dll
                                 C:\Windows\System32\propsys.dll
C:\Windows\System32\catsrvut.dll
  Opens:
  Opens:
  Opens:
                                 C:\Windows\System32\mfcsubs.dl1
C:\Windows\System32\sxs.dl1
  Opens:
  Opens:
                                 C:\Windows\System32\eventcls.dll
                                 C:\Windows\System32\stdole2.tlb
C:\Windows\System32\msxm13.dl1
  Opens:
  Opens:
  Opens:
                                 C:\Windows\System32\en-US\KernelBase.dll.mui
C:\Windows\System32\msxm13r.dll
  Opens:
  Opens:
                                 C:\Windows\Svstem32\wintrust.dll
                                 C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-
00C04FC295EE}\catdb
Opens:
00C04FC295EE}\catdb
                                 C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-
  Opens
                                 C:\Windows\Svstem32\catroot2\edb.chk
  Opens
                                 C:\Windows\System32\sdclt.exe
C:\USERS\ADMIN\APPDATA\ROAMING\MICROSOFT\WINDOWS\COOKIES\ADMIN\@DEMDEX[2].TXT

Opens: C:\USERS\ADMIN\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET
FILES\CONTENT.IE5\KQ5TVCON\LOCALE-SPECIFIC[1].CSS

Opens: C:\Windows\Fonts\palab.ttf
                                 C:\WINDOWS\SYSTEM32\CATROOT\TMP1E1E.TMP
  Opens:
  Opens:
                                 C:\WINDOWS\SYSTEM32\CATROOT\TMP1E09.TMP
C:\WINDOWS\SOFTWAREDISTRIBUTION\WUREDIR\9482F4B4-E343-43B6-B170-
  Opens:
9A65BC822C77\WIREDTR CAR BAK
                                 C:\WINDOWS\SYSTEM32\CATROOT\TMP26E3.TMF
  Opens:
  Opens:
                                 C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
  Opens:
                                 C:\Windows\System32\wersvc.dll
C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
  Opens:
  Opens:
                                 C:\CONFIG MST
                                 C:\CONFIG.MSI\41EA3.RBF
  Opens:
  Opens:
                                 C:\CONFIG.MSI\41F56.RBF
  Opens:
                                 C:\Windows\System32\wiaservc.dll
C:\Windows\System32\msv1_0.dll
  Opens:
  Opens:
                                 C:\CONFIG.MSI\41F57.RBF
                                 C:\Windows\System32\wiatrace.dll
  Opens
                                 C:\Windows\debug\WIA\wiatrace.log
C:\Windows\System32\drivers\nwifi.sys
C:\Windows\AppPatch\drvmain.sdb
  Opens:
  Opens:
  Opens:
Writes to:
                                 C:\Windows\System32\drivers\ndisuio.sys
C:\Windows\System32\output.txt
  Writes to:
                                 C:\Windows\System32\Msdtc\Trace\dtctrace.log
                                 C:\Windows\System32\Msdtc\MSDTC.LOG
  Writes to:
Writes to:
{\tt C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new} \\
  Writes to:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Writes to:
C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Writes to:
C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
                                 C:\Windows\System32\output.txt
   Reads from
                                 C:\Windows\Fonts\StaticCache.dat
  Reads from:
  Reads from:
                                 C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
   Reads from
\verb|C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst| \\
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
                                 C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
  Reads from:
Network Events
```

Opens:

C:\Windows\Fonts

TVCCVVOTR EVENCS		
DNS query:	WPAD	
DNS query:	WORKGROUP	
DNS query:	MSBROWSE	
DNS query:	WORKGROUP	
Connects to:	10.74.10.255:137	
Connects to:	10.74.10.255:138	
Sends data to:	10.74.10.255:137	
Sends data to:	10.74.10.255:138	
Receives data from:	10.74.10.100:137	
Receives data from:	10.74.10.100:138	

Windows Registry Events

HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6linklocal\linklocal_ff00::%11/8 HKCU\software\classes\local settings\muicache\27\52c64b7e Creates key:

Creates kev: HKCU\software\classes\local settings\muicache

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

32c86e1ba19f}\control

Creates key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-

32c86e1ba19f}\#\control

HKLM\system\currentcontrolset\control\deviceclasses Creates key: Creates key HKLM\system\currentcontrolset\services\umbus\enum HKLM\software\classes

Creates key

Creates key HKLM\system\currentcontrolset\services\vss\diag\registry writer HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
HKLM\system\currentcontrolset\services\vss\diag\asr writer Creates key Creates key

Creates key ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ vss \verb|\ diag \verb|\ shadow \ copy \ optimization$

writer

Creates kev: HKLM\svstem\currentcontrolset\control\stillimage\trace

Creates key

HKLM\system\currentcontrolset Creates key: Creates key

HKLM\system\currentcontrolset\control HKLM\system\currentcontrolset\control\stillimage Creates key:

Creates key HKLM\svstem\currentcontrolset\control\stillimage\trace\wiaservc.dll

HKLM\system\currentcontrolset\services\nativewifip\enum
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip Creates key: Creates key: Creates key

HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000\control Creates key: Creates key HKLM\svstem\currentcontrolset\services\nativewifip\parameters Creates key: HKLM\system\currentcontrolset\services\nativewifip Creates key: $HKLM \setminus system \setminus current control \\ \\ control \\ \\ class \setminus \{4d36e972-e325-11ce-bfc1-e325-11ce-bfc$

Creates key: 08002be10318}\0005

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

08002be10318}\0008

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

08002be10318}\0006 Creates key: 08002be10318}\0007

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

Creates key: HKLM\system\currentcontrolset\services\ndisuio\en Creates key: HKLM\system\currentcontrolset\enum\root\legacy_ndisuio Creates key HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000 HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000\control Creates key: Creates key HKLM\svstem\currentcontrolset\services\ndisuio HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0000

Creates key: 08002be10318}\0003

Creates key

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

08002be10318}\0004 Creates key:

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

08002be10318}\0002 Creates key: 08002be10318}\0001

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

Creates key: 08002be10318}\0011

Creates key: 08002be10318}\0009

Deletes value HKI M\system\currentcontrolset\services\umbus\enum[1] Opens key: HKLM\system\currentcontrolset\control\session manager Opens kev: HKLM\svstem\currentcontrolset\control\terminal server Opens key: Opens key: HKLM\system\currentcontrolset\control\safeboot\option
HKLM\system\currentcontrolset\control\srp\gp\dll

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

Opens key: HKCU\ Opens key:

HKCU\control panel\desktop\muicached\machinelanguageconfiguration

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

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

HKCU\control panel\desktop\muicached
HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ sorting \verb|\ versions| \\$

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

Opens key: HKLM\software\microsoft\rpc
HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key:

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

Opens kev: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows
HKLM\system\currentcontrolset\control\sqmservicelist Opens key:

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

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

Opens key: HKLM\software\microsoft\ole

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

HKLM\software\microsoft\com3
HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da} Opens key: Opens key: Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\treatas HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\progid Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprocserver32 Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler32 HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler

Opens kev: Opens key: HKCR\appid\alg.exe

HKLM\software\microsoft\ole\appcompat Opens key: Opens key HKLM\svstem\currentcontrolset\control\lsa

Opens key HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

Opens key:

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

 $\label{thklm} HKLM \system \current control set \policies \microsoft \cryptography \configuration \\ Opens \ensuremath{\mbox{ Opens key:}} HKLM \software \policies \microsoft \cryptography$

Opens kev: Opens key:

HKLM\software\microsoft\cryptography
HKLM\software\microsoft\cryptography\offload
HKCR\interface\{00000134-0000-0000-c000-000000000046} Opens key: Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32

Opens key: HKLM\software\microsoft\rpc\extensions Opens key: HKLM\svstem\currentcontrolset\services\bfe

HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key

```
Opens key
                                           HKLM\software\microsoft\sqmclient\windows\disabledsessions\
                                           HKCR\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
   Opens key:
   Opens key:
   Opens key:
                                            HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1
   Opens key:
                                           HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
  Opens key:
  Opens key:
Opens key:
                                           HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
  Opens key
                                            HKCR\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
   Opens key:
                                            HKLM\software\microsoft\alg\isv
  Opens key:
                                            HKLM\software\microsoft\msdtc\tracing
                                           HKLM\software\microsoft\msdtc\tracing\sources
HKLM\software\microsoft\msdtc\tracing\output
   Opens key:
   Opens key:
   Opens key
                                            HKI M\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
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\description
   Opens key:
   Opens key:
  Opens key:
                                           HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\description
  Opens key:
                                            HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5
                                           HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5\description
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9
   Opens key:
   Opens key:
  Opens key:
                                           \label{localbound} HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\\ \description \ HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed
  Opens key:
                                            HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\description
   Opens key:
                                            HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid
                                            HKCR\svcid.local
   Opens key:
  Opens key:
                                            HKCR\svcid local\488091f0-bff6-11ce-9de8-00aa00a3f464
                                           HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\nost
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\clsid
  Opens key:
                                           \label{eq:hkcrsvcid.local} HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider\\ HKCR\cid.local\4777da18-5d11-4ac9-b6c0-782ab52d45ed\protocol
   Opens key:
                                           HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\endpoint
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\customproperties
   Opens key:
   Opens key:
  Opens key:
                                           HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\customproperties\log
Opens key: HKCR\cid.local
782ab52d45ed\customproperties\log\size
                                            HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
  Opens key:
Opens key:
                                           HKLM\software\microsoft\msdtc\mtxoci
HKLM\software\microsoft\msdtc\security
  Opens key:
                                           HKLM\software\microsoft\windows nt\currentversion\asr\restoresession
                                            HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
782ab52d45ed\customproperties\log\path
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions
  Opens key:
                                           HKLM\svstem\currentcontrolset\control\minint
                                           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 key:
  Opens key:
                                           HKLM\svstem\currentcontrolset\control\nls\customlocale
                                           Opens key:
   Opens key
   Opens key:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:
Opens key:
                                           HKLM\software\microsoft\ctf\
HKLM\software\microsoft\ctf\knownclasses
\label{lem:openskey:} Openskey: \\ \mbox{HKLM} software \mbox{microsoft} windows \current version \side by side \as sembly storage roots \end{substitute} % \label{lem:openskey:microsoft} % \mbox{windows} \columnwidth \columnw
  Opens kev:
                                           HKLM\software\microsoft\windows\windows error reporting\wmr
   Opens key:
                                           HKLM\software\microsoft\directui
HKLM\system\currentcontrolset\control\nls\locale
   Opens key:
   Opens key:
                                           HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
                                            HKLM\system\currentcontrolset\control\nls\language groups
   Opens key:
   Opens kev:
                                           HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
                                           HKLM\software\microsoft\windows
   Opens key
nt\current version\language pack\datastore\_v1.0
Opens key: HKLM\software\microsoft nt\currentversion\languagepack\surrogatefallback
                                           HKLM\software\microsoft\windows
                                           HKLM\software\microsoft\windows
  Opens kev:
nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKLM\system\currentcontrolset\control\timezoneinformation
   Opens key
                                           \label{thm:loss} HKLM \software \microsoft \windows nt\current version \tracing \mbox{$\mbox{modules}$} HKLM \software \mbox{$\mbox{$\mbox{$microsoft}$} \sin dows }
   Opens key
nt\currentversion\tracing\msdtc\modules\transaction_transitions
   Opens key:
                                           HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed HKLM\software\microsoft\windows nt\currentversion
   Opens key:
   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
   Opens key:
                                           HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\clsid
HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
  Opens key:
  Opens key:
Opens key:
                                           \label{thm:hkkcr} HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\\ HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\\ \end{tabular}
                                           HKCU\control panel\international HKLM\software\microsoft\rpc\securityservice
  Opens key:
   Opens key:
                                            HKLM\svstem\currentcontrolset\control\lsaextensionconfig\sspicli
  Opens key:
  Opens key:
Opens key:
                                           HKLM\system\currentcontrolset\control\securityproviders
                                           HKLM\system\currentcontrolset\control\fas\spicache\credssp.dll

HKLM\system\currentcontrolset\control\fas\spicache\credssp.dll

HKCN\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\customproperties
  Opens kev
   Opens key:
  Opens key:
  Opens key:
Opens key:
                                           HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\customproperties\dac
  Opens kev
                                            HKLM\svstem\currentcontrolset\services\ldap
   Opens key:
                                            HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\svcid
                                            HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef
  Opens key:
                                           HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\host
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\clsid
   Opens key:
   Opens key:
   Opens key
                                            HKCR\svcid local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider
                                           HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol
   Opens key:
  Opens key:
                                           HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\svcid
HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
   Opens key:
   Opens key:
   Opens key
                                            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:
                                            HKLM\software\microsoft\windows nt\currentversion\svchost
   Opens key:
                                            HKLM\software\microsoft\windows
nt\currentversion\svchost\localservicepeernet
```

HKLM\system\currentcontrolset\services Opens key:

```
Opens kev:
                  HKLM\svstem\currentcontrolset\services\p2pimsvc
                 HKLM\system\currentcontrolset\services\p2pimsvc\parameters
HKLM\software\microsoft\windows nt\currentversion\winlogon
 Opens key:
 Opens key:
 Opens key:
                  HKLM\software\policies\microsoft\windows\system
                  HKLM\software\policies\microsoft\peernet
 Opens key:
 Opens kev:
                  HKLM\svstem\currentcontrolset\services\pnrpsvc
 Opens key:
                  HKLM\system\currentcontrolset\services\pnrpsvc\parameters
                  HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
 Onens key
                  HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog\2c69d9f1-3a1fc5ac
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
Opens kev:
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
 Opens key:
 Opens key:
                  HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
                  HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000000
 Opens key:
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
 Opens key:
 Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000011
                 HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
 Opens key:
 Opens key:
Opens key:
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 key: 
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
 Opens kev:
HKLM\system\currentcontrolset\control\computername
Opens key:
 Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000018
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\0000000c
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock\parameters
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key:
Opens key:
 Opens kev:
                  HKLM\system\currentcontrolset\services\winsock\setup migration\providers
                  HKLM\system\currentcontrolset\services\winsock\setup
 Opens key
migration\providers\tcpip6
 Opens key:
                 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens kev
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
Opens key:
c19ce8a73253}
806e6f6e6963}
Opens key:

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

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
                                     HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:
   Opens key
                                     HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0
   Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
   Opens key
                                     \label{thm:local} HKLM \system \current controls exist manager \environment \\ HKLM \system \current version \\
   Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
  Opens key:
   Opens key:
                                     HKCU\environment
                                     HKCU\volatile environment
   Opens key:
  Opens key:
                                     HKCU\volatile environment\0
                                      HKLM\software\policies\microsoft\windows\explorer
   Opens key:
  Opens kev:
                                     HKCU\software\policies\microsoft\windows\explorer
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
HKLM\software\microsoft\miss.

9afe-ea3317b67173}\propertybag

Opens kev: HKLM\system\currentcontrolset\services\crypt32
   Opens key:
                                     HKLM\software\microsoft\cryptography\oid
HKLM\software\microsoft\cryptography\oid\encodingtype 0
   Opens key:
  Opens key:
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
0\certdllopenstoreprov\#16
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
0\certdllopenstoreprov\ldap
                                     HKLM\software\microsoft\cryptography\oid\encodingtype 1
   Opens key:
  Opens key:
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
                                     {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype}
  Opens key
0\cryptdlldecodeobjectex
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
Opens key:
1\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\c \\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
                                     {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
                                     HKLM\software\microsoft\crvptography\oid\encodingtype
  Onens key
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
                                     {\tt HKLM \ } software \verb|\ microsoft \ \\ cryptography \verb|\ oid \ \\ encoding type \\
1\crvptdlldecodeobjectex\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
                                     {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
                                     HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens kev:
   Opens key:
                                     HKLM\software\microsoft\cryptography\defaults\provider types\type 012 HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
  Opens key:
schannel cryptographic provider
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}\propertybag
                                     HKLM\software\microsoft\cryptography\deshashsessionkeybackward
  Opens key:
Opens key:
0\cryptdllfindoidinfo
                                      HKLM\software\microsoft\cryptography\oid\encodingtype
                                     {\tt HKLM \coftware \microsoft \cryptography \coid \encoding type}
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7
  Opens kev:
                                     HKLM\svstem\currentcontrolset\control\mui\stringcachesettings
   Opens key:
                                     HKCU\software\classes\local settings\muicache\27\52c64b7e
  Opens key:
  Opens key:
                                     HKLM\svstem\currentcontrolset\control\deviceclasses
                                      HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#\65a9a6cf-64cd-480b-843e-
32c86e1ba19f}
   Opens key:
                                      HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
32c86e1ba19f}\#
                                     HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
  Opens key:
b082-00a0c91efb8b}
Opens key:
b082-00a0c91efb8b}\##?
                                     HKLM\svstem\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-
00a0c91efb8b}
HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&080#{2accfe60-c130-11d2-b082-00a0c91efb8b}
                                     HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
  Opens kev:
b082-00a0c91efb8b\} \verb||| \#?|| pciide|| idechannel|| \#4&2ab44545&0&1|| \#2accfe60-c130-11d2-b082-00a0c91efb8b\}|| \#2accfe60-c130-11d2-b082-00a0c91efb8b||| #2accfe60-c130-11d2-b082-00a0c91efb8b||| #2accfe60-c130-00a0c91efb8b||| #2accfe60-c1
                                     HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
  Opens kev:
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2d9c6e01&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b\\##?#pciide#idechannel#4&2f42c713&0&0#{2accfe60-c130-11d2-b082-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11b082-00a0c91efb8b}\\##?#pciide#idechannel#4&2f42c713&081#{2accfe60-c130-11d2-b082-00a0c91efb8b}
                                     HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
Opens key:
84ae-d30803bae505}
                                     HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
  Opens key
                                     HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
84ae-d30803bae505}\##?#
                                    oot#vdrvroot#0000#{2e34d650-5819-42ca-84ae-d30803bae505}
                                     HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
  Opens key:
bc8c-00a0c91405dd}
                                     HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
  Opens key:
bc8c-00a0c91405dd}\##?#acpi#pnp0f03#481d401fb580#1378de44c-56ef-11dl-bc8c-00a0c91405dd}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11dl-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&co102#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-
00a0c91405dd}
                                     HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
  Opens key:
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&1e20eb37&0&0001#{378de44c-56ef-11d1-bc8c-
00a0c91405dd}
  Opens key:
                                     HKLM\svstem\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col03#6&1c83c2e&0&0002#{378de44c-56ef-11d1-bc8c
```

00a0c91405dd} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-bc8c-00a0c91405dd}\#;?#hid#vid_14dd&pid_1005&col03#6&1e20eb37&0&0002#{378de44c-56ef-11d1-bc8c-00a0c91405dd} Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{3bc8c-00a0c91405dd}\##?#root#rdp_mou#0000#{378de44c-56ef-11d1-bc8c-00a0c91405dd} Opens key: 8a92-1e6861e6af27} HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Opens key HKI M\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c8&subsys_01e61028&rev_01#3&2411e6fe&0&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\\##?#pci#ven_8086&dev_27c8&subsys_01e61028&rev_01#3&2411e6fe&1&e8#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-4\ 8a92-1e6861e6af27\\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&0&e9#{3abf6f2d-HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-71c4-462a-8a92-1e6861e6af27} HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-Opens key: 8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&1&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens kev: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&0&ea#{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-46 8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27ca&subsys_01e61028&rev_01#3&2411e6fe&1&ea#{3abf6f2d-HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\\##?\pci\ven_8086\dev_27cc\subsys_01e61028\rev_01\#3\&2411e6fe\&0\&ef\{3abf6f2d-71c4-462a-8a92-1e6861e6af27} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-46 8a92-1e6861e6af27}\##?#pci#yen_8086&dev_27cc&subsys_01e61028&rev_01#3&2411e6fe&1&ef#{3abf6f2d-HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-71c4-462a-8a92-1e6861e6af27} HKLM\system\currentcontrolset\control\deviceclasses\{4116f60b-25b3-4662-Opens key: b732-99a6111edc0b} Opens key: a5d6-28db04c10000} HKLM\svstem\currentcontrolset\control\deviceclasses\{4747b320-62ce-11cf-Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{ a5d6-28db04c10000} \##?#root#system#0000#{4747b320-62ce-11cf-a5d6-28db04c10000} Opens key: be5e-00a0c9062857} HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-Opens kev: HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0be5e-00a0c9062857}\##?#acpi#fixedbutton#2&daba3ff&0#{4afa3d53-74a7-11d0-be5e-00a0c9062857} HKLM\system\currentcontrolset\control\deviceclasses\{4afa3d53-74a7-11d0-Opens key: $Opens\,key: \qquad \qquad \text{HKLMN-system} \\ \text{tontrol-set} \\ \text{control-device} \\ \text{color-good-second} \\ \text{tond-secon$ Opens key: 88cb-001111000030} HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-1' 88cb-001111000030}\\##?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030} 001111000030} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-88cb-001111000030}\##?#hid#vid_14dd&pid_1005&col02#6&1c83c2e&0&0001#{4d1e55b2-f16f-11cf-88cb 001111000030} Opens key: HKLM\system\currentcontrolset\control\devicecidsses\tquiessus\tqu

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

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

88cb-001111000030}\##?#hid#vid_14dd&pid_1005&co103#6&1c83c2e&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-88cb-00111100030}\#;?#hid#vid_14dd&pid_1005&col03#6&1e20eb37&0&0002#{4d1e55b2-f16f-11cf-88cb-001111000030}

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

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

#ide#diskvbox_harddisk __#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b} Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d 94f2-00a0c91efb8b}\##?#scsi#disk&ven_dell&prod_virtual_disk#6&17b13437&0&000000#{53f56307-b6bf- $HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f56307-b6bf-11d0-b6b$

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

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

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

Opens key: https://de/carbmil-dt-st_dvd-rom_gdrt100_______1.02____#5&28836b88&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: httln://dvd-rom_gdrt100________1.05____#5&28836b88&0&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
##?#ide#cdromhl-dt-st_dvd-rom_gdrt100________1.05____#5&23a61b2180&0.0.0#{53f56308-b6bf-11d0-94f2-00a0c91efb8b}

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

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

94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-rom_ 00a0c91efb8b}

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

9472-00a0c91erb88}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdrt10n______1.02___#5828836b880&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

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

__1.05___#5823a61b2180&0.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0t10n_ Opens key: 94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-

__1.0__ _#5&106af171&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

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

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

rom 00a0c91efb8b}

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

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

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

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\device 94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-806e6f6e6963}#0000002131c36800#{53f5630d-b6bf-11dd-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#;?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#00000000000000000000#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}

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

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

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\
94f2-00a0c91efb8b\\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000002131c36800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot1#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot10#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?\storage\volumesnapshot\harddiskvolumesnapshot11\#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{53f5630d-b6bf-11c94f2-00a0c91efb8b}\\##?\#storage\#volumesnapshot\#harddiskvolumesnapshot2\#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?\#storage\#volumesnapshot\#harddiskvolumesnapshot2\#\#\fac{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##?\#storage\#volumesnapshot\#harddiskvolumesnapshot2\#\fac{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\##\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fac{7}{2}\#\fa
                                                          00a0c91efb8b}
HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11c94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2-
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
00a0c91efb8b}
Opens kep: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\\#?#storage#volumesnapshot#harddiskvolumesnapshot6#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d 94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-
                                                          00a0c91efb8b}
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
    Opens key:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot8#{53f5630d-b6bf-11d0-94f2
00a0c91efb8b}
    Opens key:
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key:
94f2-00a0c91efb8b}
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
    Opens kev:
94f2-00a0c91efb8b}\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
   Opens key:
85bb-30ff1f953599}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\control\deviceclasses\con
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
f2f2-4f3b-85bb-30ff1f953599}
                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
    Opens kev:
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.117
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
Opens key: HKLM\system\currentcontrolset\control\u00e4\cectasses\\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\\00075500\cdot\00075500\cdot\\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\00075500\cdot\000755
 f2f2-4f3b-85bb-30ff1f953599}
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
   Opens key:
85bb-30ff1f953599}\##?#pci#ven_80ee&dev_beef&subsys_00000000&rev_00#3&267a616a&0&10#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}
                                                        HKIM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}\##?#root#umbus#0000#{65a9a6cf-64cd-480b-843e-32c86e1ba19f}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cт-b
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
32c86e1ba19f}\#\control
Opens key:
bcf7-00aa00b7b32a}
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
   Opens key:
bcf7-00aa00b7b32a}\##?#acpi#pnp0c0a#0#{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
a537-0000f8753ed13
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f72a537-0000f8753ed1}\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-
```

0000f8753ed13

```
Opens kev:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
   Opens key:
b7df-24c5d8a8ccb8}\##?#display#default_monitor#4&2abfaa30&0&12345678&00&02#{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}
   Opens kev:
                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}
   Onens key
                                            HKI M\system\currentcontrolset\control\deviceclasses\{866519h5-3f07-4c97-
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 key: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-bc8c-00a0c91405dd}\##?#acpii#pnp0303#4&1d401fb5&0#{884b96c3-56ef-11d1-bc8c-00a0c91405dd}
                                            HKI M\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
  Opens key:
                                            HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c
00a0c91405dd}
Opens key: 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}
Opens key:
af1f-0000f800845c}
                                            Opens key:
                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
af1f-0000f800845c}\##?#acpi#pnp0400#4&1d401fb5&0#(97f76ef0-f883-11d0-af1f-0000f800845c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
359c-8bef029dbdd01
Opens key: HKLM\system\currentcontrolset\control\de 359c-8bef029dbdd0}\##?#acpi#genuineintel_-_x86_family_6_model_15_
                                            HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
                                                        _x3220__@_2.40ghz#_1#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
_intel(r)_xeon(r)_cpu_
                                            HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
  Opens key:
359c-8bef029dbdd0}\##?#acpi#genuineintel_-_x86_family_6_model_15_-
_intel(r)_xeon(r)_cpu____x3220_@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-8bef029dbdd0}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\\97fadb10-4e33-40ae-359c-8bef029dbdd0\\\##?#acpi#genuineintel_-_x86_family_6_model_15_-_intel(r)_xeon(r)_cpu____x3220_@_2.40ghz#_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_-
_intel(r)_xeon(r)_cpu___x3220_@_2.40ghz#_4#{97fadb10-4e33-40ae-359c-8bef029dbdd0}\\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-
Opens key:
901f-00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34a9bc#{a5dcbf10-6530-11d2-901f-
00c04fb951ed}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\\##?#usb#vid_14dd&pid_1005#fac72212e15ea84#{a5dcbf10-6530-11d2-901f-
00c04fb951ed}
Opens key:
8dcb-00c04fc3358c}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11dt
8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{ad498944-
                                            HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
762f-11d0-8dcb-00c04fc3358c}
                                           HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Opens key:
8dcb-00c04fc3358c}\##?#pci#yen 14e4&dev 1659&subsys 01e61028&rev 11#4&27c84f55&0&00e4#{ad498944
762f-11d0-8dcb-00c04fc3358c)
                                          HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Opens kev:
8dcb-00c04fc3358c}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad498944-
762f-11d0-8dcb-00c04fc3358c}
                                           HKI M\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#*isatap#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
                                           HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Opens key:
8dcb-00c04fc3358c}\##?#root#*teredo#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_agilevpnminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLMNsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms 12tpminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#ms_ndiswanbh#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
\label{lem:openskey: HKLMN-system-current controlset-control-device classes {ad498944-762f-11d0-8dcb-00c04fc3358c} \\ \text{#?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c} \\ \text{The control open sey: } \text{The contro
                                           HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
  Opens key:
8dcb-00c04fc3358c}\##?#root#ms_ndiswanipv6#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb-00c04fc3358c}
Opens key: HKLMNsystem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}
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}
\label{lem:openskey: HKLMN-system-current} Opens key: $$HKLMN-system-currentcontrol-set-control-deviceclasses-{ad498944-762f-11d0-8dcb-00c04fc3358c}$$ HKLMN-system-would-fad498944-762f-11d0-8dcb-00c04fc3358c}$$
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-118dcb-00c04fc3358c}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{ad498944-762f-11d0-8dcb-00c04fc3358c}
                                           HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
Opens key:
82e6-71a87abac361}
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
  Opens kev:
                                           HKLM\svstem\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}
Opens key: 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}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c82e6-71a87abac361}\#?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c8266-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c8266-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_01e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c8266-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_01e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c8266-71a87abac361}\##?#pci#ven_8086&dev_100e&subsys_01e8086&rev_02#3&267a616a&0&18#{cac88484-7515-4c8266-71a87abac361}\##
                                            HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
7515-4c03-82e6-71a87abac361}
                                           HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\##?#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87abac361}\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\\##?\root\ms_agilevpnminiport\ms_0000\frac82e6-71a87abac361}\\\ms_agilevpnminiport\ms_0000\frac82e6-71a87abac361}
                                           HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_l2tpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                           HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
   Opens key
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_ndiswanipv6#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
Openskey: HKLMNsystem\currentcontrolset\control\deviceclasses\{cac88484-82e6-71a87abac361}\#?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-71a87abac361}
                                           HKLM\svstem\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}\##?#sw#{eeab7790-c514-11d1-b42b-00805fc1270e}#asyncmac#{cac88484-7515-4c03-
82e6-71a87abac361}
   Opens key:
                                                         HKLM\svstem\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
 ac88-96b894c191e2}
   Opens key:
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{e849804e-c719-43d8-
ac88-96b894c191e2}\##?#acpi#pnp0c0a#0#{e849804e-c719-43d8-ac88-96b894c191e2}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
hcaa-942h189880983
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-bcaa-942b18988098}\##:#usb#root_hub#4&152cc752&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
                                                         Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-bcaa-942b18988098}\##?#usb#root_hub#4822939226&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
\label{lem:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key:open-key
   Opens key
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
bcaa-942b18988098}\##?#usb#root_hub20#4&305beb51&0#{ed8cf6b1-62d5-4597-bcaa-942b18988098}
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
    Opens key:
8815-00a0c906hed83
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-
8815-00a0c906bed8}\##?#usb#root_hub#4&13571ab5&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
                                                         Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
\label{lem:openskey: HKLMN-system-current} Opens key: $$HKLMN-system-currentcontrol-set-control-deviceclasses $$\{f18a0e88-c30c-11d0-8815-00a0c906bed8\} $$\
    Opens kev:
                                                        HKLM\svstem\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&24693ec3&0#{f18a0e88-c30c-11dd-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11dd-
8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub20#4&211f73e0&0#\\f18a0e88-c30c-11d0-8815-00a0c906bed8\
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\\ff18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub20#4&305beb51&0#\\ff18a0e88-c30c-11d0-8815-00a0c906bed8\\
    Opens kev:
                                                        HKLM\svstem\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-8815-00a0c906bed8}\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#{f18a0e88-c30c-11d0-8815-00a0c906bed8}
\label{lem:openskey: https://linear.properties.properties.} Openskey: $$HKLM\system\currentcontrolset\enum\umb\umb\18841921d\&0&printerbusenumerator.$$
                                                         HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
    Opens key
08002be10318}
    Opens key:
                                                         HKLM\system\currentcontrolset\services\umbus
    Opens key
                                                         0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
    Onens key
Opens key: https://doi.org/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.1001/10.
Opens key: HKLM\software\microsor0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllencodepublickevandparameters
Opens key: HKLM\software 1\cryptdllencodepublickeyandparameters
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllencodeobjectex
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
    Opens key
1\cryptdllencodeobjectex
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
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
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.11
                                                        {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid \backslash encoding type}
 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.12
                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
    Opens key:
Opens key: httl://openskey: httl://opens
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\w:
                                                         HKLM\software\microsoft\windows\currentversion\setup
                                                         HKLM\system\currentcontrolset\control\print
    Opens key:
    Opens key:
                                                         HKCR\clsid
    Opens key:
                                                         HKLM\software\policies\microsoft\windows nt\printers
    Opens kev:
                                                         HKLM\svstem\currentcontrolset\services\lanmanworkstation\parameters
    Opens key:
                                                         HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
                                                         HKCR\appid\vssvc.exe
    Opens key:
                                                        HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}

HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\treatas

HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid
    Opens key:
    Opens key:
    Opens key:
    Opens key:
                                                         HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprocserver32
HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
    Opens key:
    Opens key:
Opens key:
                                                         HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
                                                         HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\treatas
    Opens key:
                                                        HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprocserver32
    Opens key:
    Opens key:
                                                         HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler32
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler
    Opens key:
    Opens key:
    Opens key:
                                                         HKLM\svstem\currentcontrolset\services\vss\settings
                                                         HKLM\system\currentcontrolset\services\vss\diag
    Opens key:
    Opens key:
                                                         HKLM\system\currentcontrolset\services\vss\diag\registry writer
                                                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
    Opens key:
    Opens key:
    Opens kev
                                                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid
    Opens key:
                                                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
    Opens key:
                                                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
    Opens key:
    Opens key:
    Opens key
                                                         HKCR\clsid\{1he1f766-5536-11d1-h726-00c04fh926af}\treatas
                                                         HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\progid
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\nprocserver32
    Opens key:
    Opens key:
                                                        HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler
    Opens key:
    Opens key:
    Opens key
                                                         HKCR\interface\{64h8f404-a4ae-11d1-h7h6-00c04fh926af}
    Opens key:
                                                         HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32
                                                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
    Opens kev:
                                                        HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\progid
    Opens key:
    Opens key:
    Opens key
                                                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
    Opens key:
                                                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
    Opens key:
                                                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler
                                                         HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}
```

```
HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
   Opens key:
                                           HKCR\interface\{00000100-0000-0000-c000-00000000046}\
HKCR\interface\{00000100-0000-0000-c000-00000000046}\
proxystubclsid32
   Opens key:
   Opens key:
   Opens key:
                                           HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}
   Opens key:
                                           HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
HKCR\clsid\{7542960-79c7-11d1-88f9-0080c7d771bf}
   Opens key:
                                           HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid
   Opens key:
   Opens key:
   Opens key
                                           HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32
                                           HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler32
   Opens key:
   Opens key:
                                           HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}
HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
   Opens key:
   Opens key:
   Opens key
                                           \label{thm:local-hklm} HKLM \system \current control set \services \vss \diag \com+ regdb \writer \end{tabular} writer \\ HKLM \system \current control set \services \vss \diag \com+ regdb \writer \end{tabular} writer
   Opens key:
  Opens key:
                                           {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ vss \verb|\ diag \verb|\ shadow \ copy \ optimization \\
   Opens key:
                                           HKCR\interface\{0000000c-0000-0000-c000-00000000046}
   Opens key:
                                           Opens key:
                                           HKLM\svstem\currentcontrolset\services\wersvc
                                           HKLM\system\currentcontrolset\services\wersvc\parameters
HKLM\software\microsoft\windows\windows error reporting
   Opens key:
   Opens key:
   Opens key:
                                           HKLM\software\microsoft\windows nt\currentversion\svchost\imgsvc
HKLM\system\currentcontrolset\services\stisvc
   Opens key:
                                           HKLM\system\currentcontrolset\services\stisvc\parameters
   Opens key:
                                            HKLM\system\currentcontrolset\control\stillimage\trace
                                           HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll
   Opens key:
   Opens key:
                                           HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
   Opens key:
                                           HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\treatas
                                           HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\progid
HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprocserver32
   Opens key:
   Opens key:
                                           \label{local-eq:hkcrkclsid} $$HKCR\clsid_{a1f4e726-8cf1-11d1-bf92-0060081ed811}\sim HKCR\clsid_{a1f4e726-8cf1-11d1-bf92-0060081ed811}\sim HKCR_{a1f4e726-8cf1-11d1-bf92-0060081ed811}\sim HKCR_{a1f4e726-8cf1-11d1-bf92-0060081ed811}
   Opens key:
                                           HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
                                           HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\treatas
HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\progid
   Opens key:
   Opens key:
   Opens key:
                                           HKCR\clsid\\b6c292bc-7c88-41ee-8b54-8ec92617e599\\inprocserver32
HKCR\clsid\\b6c292bc-7c88-41ee-8b54-8ec92617e599\\inprochandler32
                                           HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler
   Opens key:
                                            HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
   Opens key:
                                           HKLM\svstem\currentcontrolset\control\stillimage\fakedevices
   Opens key:
   Opens key:
Opens key:
                                           \label{thm:local_hammon} HKLM\system\currentcontrolset\control\stillimage\mbox{\scdevicelist} \\ HKLM\system\currentcontrolset\control\stillimage\mbox{\scdevicelist} \\ \label{thm:local_hammon}
   Opens key:
                                           HKLM\system\currentcontrolset\control\stillimage\events
                                            HKLM\system\currentcontrolset\control\stillimage\events\connected
   Opens key:
   Opens key:
HKLMIsystem \current control still image \events \connected \ \{38f8a702-36bb-4a68-80e6-d4966b9b718\}
                                           \label{thm:local} HKLM \system \current controls through the control still image \events \current controls the control still image \events \email image \email imag
   Opens key:
   Opens key
   Opens key:
HKLMIsystem \current control set \control still image \events \email image \d13e3f25-1688-45a0-9743-759eb35cdf9a\}
   Opens key:
                                           HKLM\svstem\currentcontrolset\control\stillimage\events\faximage
   Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
   Opens key:
                                           HKLM\system\currentcontrolset\control\stillimage\events\printimage
759eb35cdf9a3
                                           {\tt HKLM} \  \  \, \texttt{System} \  \  \, \texttt{Control} \  \  \, \texttt{Stillimage} \  \  \, \texttt{events} \  \  \, \texttt{Scanbutton}
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6
759eb35cdf9a}
Openskey:

HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}
   Opens key:
                                            HKLM\system\currentcontrolset\control\stillimage\serversettings
   Opens kev:
                                            HKLM\system\currentcontrolset\services\nativewifip
   Opens key:
                                           HKLM\system\currentcontrolset\services\nativewifip\enum
   Opens key:
                                           HKLM\system\currentcontrolset\enum\root
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000
   Opens key:
   Opens key:
   Opens key
                                           HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-
0000f8753ed1}
                                           HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-
   Opens key:
08002be10318}
                                           Opens key
08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
                                           HKLM\system\currentcontrolset\services\nativewifip\parameters
   Opens key:
                                           HKLM\svstem\currentcontrolset\services\nativewifip\filterdriverparams
   Opens key:
                                           HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
   Opens key
08002be10318}\0005\linkage
                                           HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
   Opens key:
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key
Opens key:

08002be10318}\0008\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage
   Opens kev:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
08002be10318}\0007\linkage
   Opens key:
                                           HKLM\system\currentcontrolset\services\ndisuio
   Opens kev:
                                           HKLM\system\currentcontrolset\services\ndisuio\enum
                                           HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000
HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000
   Opens key:
   Opens key:
   Opens key
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage
   Opens key:
                                           HKLM\svstem\currentcontrolset\enum\root\ms pptpminiport\0000
                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage
                                           HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
   Opens key
O8002be10318}\0004\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000
```

```
Opens key
                                               HKLM\svstem\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
Opens key:

08002be10318}\0002\linkage

Obens key:

HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000
                                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\linkage
  Opens key:
                                               HKLM\svstem\currentcontrolset\enum\root\*teredo\0000
   Opens ke
                                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\linkage
Opens key: HI
Opens key: HI
08002be10318}\0009\linkage
                                               HKLM\svstem\currentcontrolset\enum\root\*isatan\0000
                                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                               HKLM\system\currentcontrolset\control\diagnostics\performanc
   Opens key:
                                               HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
   Opens key:
context logger
Queries value:
                                               HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
   Queries value:
                                               HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
                                               HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Queries value:
   Oueries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Oueries value:
                                               HKCU\control panel\desktop[preferreduilanguages]
    Queries value:
                                               HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:
                                                HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
                                               HKLM\system\setup[systemsetupinprogress]
HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
   Oueries value:
    Queries value:
   Queries value:
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
   Oueries value:
                                               HKLM\software\microsoft\windows nt\currentversion\compatibilitv32[alg]
                                               HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
HKLM\system\currentcontrolset\control\config[system]
    Queries value
   Queries value:
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
                                               HKLM\software\microsoft\ole[pageallocatorusesystemheap]
HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
HKLM\software\microsoft\com3[com+enabled]
   Oueries value:
    Queries value:
   Oueries value:
                                               HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
Queries value:
   Oueries value:
                                                HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Queries value
   Oueries value
                                               HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ microsoft \ strong \ microsoft \ strong \ microsoft \ strong \ microsoft \ microsoft
Cryptographic provider[type]

Oueries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:
                                               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Queries value
   Oueries value
                                               HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
    Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                                               HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
HKLM\software\microsoft\cryptography[machineguid]
HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
   Queries value:
   Queries value:
   Oueries value
   Queries value:
                                                HKLM\software\microsoft\rpc\extensions[ndroleextdll]
   Oueries value:
                                                HKLM\software\microsoft\rpc\extensions[remoterpcdll]
   Queries value:
                                               HKLM\software\microsoft\sqmclient\windows\disabledprocesses[bca9f854]
   Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
   Queries value:
                                               HKLM\software\microsoft\ole [maxxxshashcount]
HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_misc] HKLM\software\microsoft\msdtc\tracing\sources[trace_cm]
   Oueries value
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
HKLM\software\microsoft\msdtc\tracing\sources[trace_svc]
HKLM\software\microsoft\msdtc\tracing\sources[trace_gateway]
   Oueries value:
   Queries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_ui]
HKLM\software\microsoft\msdtc\tracing\sources[trace_contact]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
HKLM\software\microsoft\msdtc\tracing\sources[trace_cluster]
HKLM\software\microsoft\msdtc\tracing\sources[trace_resource]
   Oueries value:
    Queries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_tip] HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
HKLM\software\microsoft\msdtc\tracing\sources[trace_log]
HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
HKLM\software\microsoft\msdtc\tracing\sources[trace_ktmrm]
   Oueries value:
   Queries value:
   Queries value:
   Queries value:
Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\sources[trace_vssbackup]
HKLM\software\microsoft\msdtc\tracing\sources[trace_vssbackup]
HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon]
HKLM\software\microsoft\msdtc\tracing\sources[trace_tm]
HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
HKLM\software\microsoft\msdtc\tracing\soutput[tracefilepath]
   Oueries value:
   Queries value
   Oueries value:
   Queries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc\tracing\output[memorybuffersize]
HKLM\software\microsoft\msdtc\tracing\output[debugoutenabled]
HKLM\software\microsoft\msdtc[noparallellogflushnotification]
   Oueries value:
   Queries value:
   Oueries value:
   Queries value:
HKLM\software\microsoft\msdtc[snapshotprefertransactionstimeoutduringbackup]
   Oueries value:
                                               HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
                                                HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\misc[disabletracing]
                                               HKLM\software\microsoft\msdtc[disableterminationonheapcorruption]
HKLM\software\microsoft\msdtc[sysprepinprogress]
   Queries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\description[]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\description[]
   Oueries value
   Queries value:
   Oueries value:
                                               HKCR\cid.local\8db0c277-238b-459d-8787-fa581fe35ed5\description[]
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\description[]
   Queries value:
   Queries value:
                                                HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\description[]
   Oueries value
                                               HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid[]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\svcid[]
   Queries value:
   Oueries value:
                                               HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\clsid[]
HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
   Queries value:
   Queries value:
                                               HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\protocol[]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-782ab52d45ed\endpoint[]
   Oueries value
   Queries value
   Oueries value:
                                               HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
```

782ab52d45ed\customproperties\log\size[]

```
Oueries value:
                                             HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
                                             HKLM\software\microsoft\msdtc\mtxoci[oraclesql1ib]
HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
   Oueries value
   Queries value:
   Oueries value
                                             HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
                                             HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
   Queries value
  Oueries value
                                             HKLM\software\microsoft\msdtc\securitv[accountname]
                                             HKLM\software\microsoft\msdtc\security[networkdtcaccess]
HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
   Queries value:
   Queries value:
                                             HKLM \software \microsoft \msdtc \security [network dtcaccess clients] \\ HKLM \software \microsoft \msdtc \security [network dtcacces stransactions] \\
   Oueries value
   Queries value
  Oueries value:
                                             HKLM\software\microsoft\msdtc\securitv[networkdtcaccesstip]
                                             HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
HKLM\software\microsoft\msdtc\security[xatransactions]
   Queries value:
   Queries value:
                                             HKLM\software\microsoft\msdtc\security[lutransactions]
HKCR\cid.local\d777da18-5d11-4ac9-b6c0-
   Oueries value
   Queries value
782ab52d45ed\customprop
                                           rties\log\path[]
Queries value:
8bd7-da8f1a74051a]
                                             HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-
  Oueries value
                                             HKI M\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
  Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxbuffers]
                                            HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\tracing\msdtc\loggingoptions[minbuffers]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[buffersize]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxfilesize]
Queries value:
nt\currentversion\compa
                                          HKLM\software\microsoft\windows
tibility32[ui0detect]
  Oueries value:
                                             HKU\.default\control panel\desktop[preferreduilanguages]
   Queries value
                                             HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
Queries value:
                                            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                                           HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-ofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
HKLM\software\microsoft\ctf[enableanchorcontext]
  Oueries value
Ofb58b01c4a4}\languagepr
  Queries value:
  Queries value:
Queries value:
                                            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Oueries value:
                                             HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries 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]
  Oueries value
                                             HKLM\software\microsoft\windo
nt\currentversion\languagepack\surrogatefallback[plane1]
  Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows
\begin{tabular}{ll} nt`currentversion\languagepack\surrogatefallback[plane3]\\ Queries value: HKLM\software\microsoft\windows \end{tabular}
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane5]
  Oueries value
                                             HKI M\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
\begin{tabular}{ll} nt`currentversion\languagepack\surrogatefallback[plane8]\\ Queries value: HKLM\software\microsoft\windows \end{tabular}
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane10]
  Oueries value
                                             HKI M\software\microsoft\window
nt\currentversion\languagepack\surrogatefallback[plane11]
  Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\langu
                                         agepack\surrogatefallback[plane12]
   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane16]
                                             HKLM\svstem\currentcontrolset\control\timezoneinformation[bias]
  Oueries value:
   Queries value:
                                            HKLM\system\currentcontrolset\control\timezoneinformation[standardname] HKLM\system\currentcontrolset\control\timezoneinformation[standardbias]
   Queries value:
  Queries value:
Queries value:
                                            HKLM\system\currentcontrolset\control\timezoneinformation[standardstart] HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\timezoneinformation[davlightbias]
                                             HKLM\system\currentcontrolset\control\timezoneinformation[daylightstart]
   Queries value
  Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[uniqueid]
Queries value: HKLM\software\microsoft\window
nt\currentversion\tracing\msdtc\modules[active]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[level]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[controlflags]
  Oueries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[uniqueid]
  Oueries 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]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
Queries value:
af58-73e332dcac8d]
                                             HKLM\system\currentcontrolset\control\wmi\security[e80aa9fe-913d-4ede-
  Oueries value
                                             HKI M\software\microsoft\msdtc[dtcmaxsessions]
   Queries value
                                             HKLM\software\microsoft\msdtc[donotgoidle]
                                             HKLM\software\microsoft\msdtc[disabletippassthrucheck]
  Oueries value:
                                             HKLM\software\microsoft\msdtc[mincheckpointinterval]
HKLM\software\microsoft\msdtc[maxcheckpointinterval]
   Queries value:
   Queries value:
                                             \label{thm:hklm:software} HKLM \software \microsoft \msdtc \security \superstands \mbox{graph} is abled] HKLM \software \mbox{microsoft} \mb
   Oueries value
   Queries value:
                                             HKLM\software\microsoft\msdtc[servertcpport]
HKLM\software\microsoft\windows nt\currentversion[currentversion]
HKLM\software\microsoft\msdtc[cmcancelrpcafter]
  Oueries value:
   Queries value:
   Queries value:
                                             HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
HKLM\software\microsoft\msdtc[cmmaxidlepings]
   Oueries value
   Queries value
  Oueries value:
                                             HKLM\software\microsoft\msdtc[cmpingfreqsecs]
                                             HKLM\software\microsoft\msdtc[cmverbose]
```

```
HKLM\software\microsoft\msdtc[rpcqosidentity]
HKLM\software\microsoft\msdtc[rpcauthnsvc]
    Queries value:
                                                            HKLM\software\microsoft\msdtc[numcccimhistoryentries]
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\svcid[]
HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\host[]
    Oueries value:
    Queries value
   Oueries value:
                                                             HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\clsid[]
HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
    Queries value:
   Queries value:
    Oueries value
                                                             HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\protocol[]
    Queries value:
                                                             HKCR\cid.local\b90b59d3-8bb9-4d71-af93-3faf363251c9\endpoint[]
   Oueries value:
                                                             HKLM\software\microsoft\msdtc[notracking]
    Queries value
                                                             HKLM\software\microsoft\rpc\securityservice[9]
    Queries value:
\label{localization} HKLM\system\corrent control\set\control\sextension config\spicli\control\sextension control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config\spicli\control\sextension config
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
    Queries value
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                                            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dl1[name] HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dl1[comment]
   Oueries value:
    Queries value
   Oueries value:
\label{thm:hamiltonian} HKLM\system \current control set \control \label{thm:hamiltonian} White \current \control \con
                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
                                                            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
    Oueries value:
    Queries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensi
   Queries value:
\label{local-problem} HKLM\system\currentcontrolset\control\set\system\currentcontrolset\services\ldap[ldap]{\label-problem} HKLM\system\currentcontrolset\services\ldap[ldap]{\label-problem}
                                                             HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Oueries value:
                                                             HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
                                                            HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\svcid[]
    Queries value:
   Queries value:
   Queries value:
Queries value:
                                                            HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\host[]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\clsid[]
   Oueries value:
                                                             HKCR\svcid.local\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider[]
                                                            HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\protocol[]
HKCR\cid.local\199661d8-979c-4ebb-9e3e-a23014be3f1a\endpoint[]
    Queries value:
    Queries value:
   Queries value:
Queries value:
                                                            HKLM\software\microsoft\msdtc[overridetiphostname]
HKLM\software\microsoft\msdtc[shared_memory_mutex_timeout]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\svcid[]
   Oueries value:
                                                            HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\host[]
HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\clsid[]
    Queries value:
    Oueries value:
    Queries value:
                                                            HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[] HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\protocol[]
    Queries value:
   Oueries value:
                                                             HKCR\cid.local\81a3a129-619d-4d5f-a782-28d960ea489d\endpoint[]
                                                             HKLM\software\microsoft\windows
    Queries value
nt\currentversion\svchost[localservicepeernet]
   Queries value:
Queries value:
                                                            HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
    Oueries value:
                                                             HKLM\software\microsoft\msdtc[transactionbridge]
    Queries value
                                                             HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
    Oueries value:
HKLMNsystem\currentcontrolset\services\p2pimsvc\parameters[servicemanifest]

Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain]
    Oueries value
                                                            HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
   Oueries value:
                                                            HKLM\software\policies\microsoft\windows\system[gpsycdebuglevel]
    Queries value:
                                                            HKLM\software\policies\microsoft\peernet[disabled] HKLM\software\microsoft\msdtc[logwarnenabled]
   Queries value:
    Oueries value
HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedllunloadonstop]
   Oueries value:
                                                            HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll]
    Oueries value
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]
                                                            HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
   Oueries value:
    Queries value:
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
    Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\software\microsoft\msdtc[suppressduplicateduration]
    Oueries value:
HKL\\ M\system\current control set\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\cute{MCM}.
   Oueries value
Queries value:
Queries value:
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
   Oueries value
Queries value:
\label{local-prop} HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000000007[packedcatalogitem]\\ Queries\ value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4\}[]
                                                            HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
HKCR\clsid\{304ce942-6e39-40d8-943a-
   Oueries value:
b913c40c9cd4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
   Oueries value:
                                                            HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
   Oueries value
Queries value:
\label{local-proposed-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000010[packedcatalogitem]
    Queries value:
HKL\\ M\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\spaces\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parameters\parame
   Oueries value
                                                            HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000012[packedcatalogitem]
    Queries value:
HKL\\ M\system\current control set\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\commont{1}{0}000000000013\\ [packed catalog item]
   Oueries value
Oueries value
```

HKLM\software\microsoft\msdtc[rpcgoscapabilities]

Oueries value:

Oueries value

Oueries value Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000017[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000018fpackedcatalogiteml Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num] Oueries value $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5 [num_catalog_entries]$ Oueries value: HKLM\software\microsoft\msdtc[supportns] Queries value: Oueries value Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001fsupportednamespace1 Queries value $HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace_catalog \\ 5 \\ catalog_entries \\ 000000000001[enabled]$ Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value: Queries value: $\label{local-prop} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]\columnwidth]{providerinfo} Queries\value:$ HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[librarypath] Queries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value: Oueries value: Queries value: Queries value: $HKLM \\ system \\ current control set \\ services \\ winsock \\ 2 \\ parameters \\ namespace_catalog \\ 5 \\ catalog_entries \\ 00000000000002 \\ [enabled]$ HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version] Oueries value: Oueries value: Oueries value: Queries value: HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003fdisplaystring7 HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003fproviderid1 Queries value: $HKL\\ M (system) current control set (services) winsock 2 (parameters) names pace_catalog 5 (catalog_entries) (000000000003 [address family]) and the system (system) (system$ 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\000000000003fyersion1 HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003fstoresserviceclassinfol Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo] Oueries value Oueries value: $HKL\\ M (system) current control set (services) winsock 2 (parameters) names pace_catalog 5 (catalog_entries) (0000000000004 [displaystring]) and the parameters of the param$ Queries value: HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004Faddressfamilv1 Queries value: $HKL\\ M\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\space]$ Oueries value Oueries value: Queries value: Oueries value $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 000000000005 [library path]$ Oueries value: $HKL\\ M (system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \nam$ Oueries value: $HKLM \ system \ current controls et \ services \ \ winsock \ 2 \ parameters \ \ namespace_catalog \ 5 \ catalog_entries \ \ \ 0000000000005 \ [providerid]$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000005[enabled] Queries value: Oueries value $HKL\\ M\system\current control set\services\winsock2\parameters\namespace_catalog5\catalog_entries\space\sp$ Oueries value: Queries value: HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006fdisplaystring7 Queries value: Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily] Oueries value: Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006fversion1

Oueries value

```
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006fstoresserviceclassinfol
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Oueries value:
Queries value:
                                                   HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
                                                   HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\s
                                                   HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
   Oueries value
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
   Oueries value:
HKLMhsystem \current control set \services \tcpip6 \parameters \winsock [helperdllname] \\ Queries \value:
\label{local-parameters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253\}[enabledhcp]}
   Oueries value:
HKLMNsystem \current control set \services \tcpip\parameters \time faces \ \{128919e8-8a5e-41d1-ac17-c19c8a73253\} [registration enabled]
   Oueries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
Queries value:
c19ce8a73253}[dhcpdomain]
   Queries value:
\label{local-prop} HKLM\system\currentcontrolset\services\tcpip6\parameters\titerfaces\{128919e8-8a5e-41d1-ac17-c19c8a73253\}[dhcpv6domain]}
   Oueries value:
806e6f6e6963}[enabledhcp]
Queries value: 
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
   Oueries value:
HKLMNsystem \current control set \services \tcpip\parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\}[dhcpdomain]
                                                   HKIM\svstem\currentcontrolset\services\tcpip\linkage[bind]
   Oueries value
                                                   HKLM\software\microsoft\sqmclient[machineid]

HKLM\software\microsoft\sqmclient[machineid]
    Queries value:
   Oueries value:
linklocal\linklocal_ff00::%11/8[seedserver]

Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
Queries value: https://disablemulticastpublish]
Queries value: https://disablemulticastpublish]
Queries value: https://disablemulticastpublish]
Queries value: HKLM\software\microsoft\window: linklocal\linklocal_ff00::%11/8[disablemulticastsearch]
Queries value: HKLM\software\nicrosoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%11/8[disabled]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%11/8[searchonly]
                                                   HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
   Oueries value:
linklocal\linklocal_ff00::%11/8[mincpalifetime]
   Queries value:
a03a-e3ef65729f3d}[category]
   Oueries value:
HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[name]
a03a-e3ef65729f3d}[parentfolder]
a03a-e3ef65729f3d}[description]
   Queries value:
a03a-e3ef65729f3d}[relativepath]
   Queries value:
a03a-e3ef65729f3d}[parsingname]
   Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \fold
a03a-e3ef65729f3d}[infotip]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localizedname]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[icon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[security]
   Oueries value:
\label{local-operator} HKLM \software \mbox{$\mathbb{K}$ indows \current version} \end{supplied} \end{supplied} AkLM \software \mbox{$\mathbb{K}$ indows \current version} \end{supplied} AkLM \software \mbox{$\mathbb{K}$ indows
a03a-e3ef65729f3d}[streamresource]
   Oueries value:
 a03a-e3ef65729f3d}[streamresourcetype]
   Queries value:
HKLM \label{eq:hkkk} Which is the statement of the stat
a03a-e3ef65729f3d}[localredirectonlv]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
 a03a-e3ef65729f3d}[roamable]
   Queries value:
a03a-e3ef65729f3d}[precreate]
   Oueries value
```

a03a-e3ef65729f3d}[stream]

Oueries value

a03a-e3ef65729f3d}[publishexpandedpath]

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

Queries value:

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

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \mbox{$microsoft$} \windows \current version \explorer \footnote{thm:local_hammon_hammo$

folders[appdata]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public] HKLM\software\microsoft\windows nt\currentversion\profilelist[default] HKLM\software\microsoft\windows\currentversion[programfilesdir] Oueries value: Queries value: Oueries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir] HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] Queries value: Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir]
HKLM\software\microsoft\windows\currentversion[commonw6432dir] Oueries value: Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19[profileimagepath]

Queries value:

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

folders[local appdata]

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

Oueries value:

 $\label{thm:hamiltonian} HKLMNsoftware \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| \{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]$

Oueries value:

 $\label{thm:local-condition} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \current \folder \current \current$ 9afe-ea3317b67173}[name]

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

9afe-ea3317b67173}[description]

Oueries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \cite{tabular} folder \cite{tab$ 9afe-ea3317b67173}[relativepath]

Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{5e6c858f-0e22-4760-164e1\} \setminus \{5e6c858f-0e22-4660-164e1\} \setminus \{5e6c858f-0e22-4660-164e1\} \setminus \{5e6c858f-0e22-4660-164e1\} \setminus \{5e6c858f-0e22-4660-1646$

9afe-ea3317b67173}[parsingname]

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

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

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

9afe-ea3317b67173}[icon] 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}[security]

Oueries value: $\label{thm:continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folds \folds$

9afe-ea3317b67173}[streamresource]

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

9afe-ea3317b67173}[streamresourcetype]

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

9afe-ea3317b67173}[localredirectonly] Queries value:

9afe-ea3317b67173}[roamable]

Oueries value:

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

9afe-ea3317b67173}[stream]

9afe-ea3317b67173}[publishexpandedpath]

Queries value:

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

Queries value:

9afe-ea3317b67173}[foldertypeid]

Oueries value:

9afe-ea3317b67173}[initfolderhandler]

Queries value:

HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
HKLM\software\microsoft\cryptography\defaults\provider types\type Queries value: 012[name]

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

schannel cryptographic provider[type] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa

schannel cryptographic provider[image path]

Oueries value: $\label{thm:condition} \begin{tabular}{ll} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\folderde$

a9dd-070d1d495d97}[category]

Queries value:

a9dd-070d1d495d97}[name]

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

a9dd-070d1d495d97}[parentfolder]

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

Oueries value:

a9dd-070d1d495d97}[relativepath]

Oueries value:

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

Oueries value:

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[infotip]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[localizedname]
    Oueries value:
a9dd-070d1d495d97}[icon]
    Oueries value:
 a9dd-070d1d495d97}[securitv]
    Queries value:
HKLM \label{eq:hkkkk} Which is the sum of 
a9dd-070d1d495d97}[streamresource]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
 a9dd-070d1d495d97}[streamresourcetype]
    Queries value:
a9dd-070d1d495d97}[localredirectonly]
   Oueries value:
a9dd-070d1d495d97}[roamable]
    Oueries value:
 HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97}[precreate]
     Queries value
HKLM \label{eq:hkkkk} Which is the sum of 
a9dd-070d1d495d97}[stream]
    Queries value:
a9dd-070d1d495d97}[publishexpandedpath]
    Queries value:
a9dd-070d1d495d97}[attributes]
   Oueries value:
a9dd-070d1d495d97}[foldertypeid]
    Oueries value:
 HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-
a9dd-070d1d495d97\} [initfolder handler] \\ Queries value: HKLM \software \policies \microsoft \cryptography [forcekey protection] \\
    Oueries value:
                                                             HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7[name]
    Queries value:
Queries value:

HKLM\system\currentcontrol\set\control\mui\stringcachesettings[stringcachegeneration]

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-
   Queries value:
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e
32c86e1ba19f}\#\control[linked]
                                                            HKLM\svstem\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
   Oueries value:
843e-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
32c86e1ba19f}\control[referencecount]
   Oueries value
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}[default]
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
   Oueries value:
b082-00a0c91efb8b\\##?
#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&37f88df1&0&400008#{2accfe60-c130-11d2-b082-
00a0c91efb8b}[deviceinstance]
                                                             HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}\##?#pci#ven_1000&dev_0054&subsys_1f091028&rev_01#5&6373acf&0&400008#{2accfe60-
c130-11d2-b082-00a0c91efb8b}{deviceinstance}

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}\##?#pciide#idechannel#4&13e1b6b&0&0#{2accfe60-c130-11d2-b082
00a0c91efb8b}[deviceinstance]
   Oueries value:
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&0#{2accfe60-c130-11d2-b082-
00a0c91efb8b}[deviceinstance]
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
    Oueries value
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2ab44545&0&1#{2accfe60-c130-11d2-b082-
00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\2accfe60-c130-11d2-b082-00a0c91efb8b\\#?#pciide#idechannel#4&2d9c6e01&0&0#\\\2accfe60-c130-11d2-b082-
DUBZ-UUJAUCFTETIODY, THE THE TENERAL TO CONTROL OF THE TENERAL THE TENER
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{2acb082-00a0c91efb8b}\\##?\pciide\pidechannel\pi4&2f42c713&0\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\text{0.80}\te
00a0c91efb8b}[deviceinstance]
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{2accfe60-c130-11d2-
   Queries value:
b082-00a0c91efb8b}\##?#pciide#idechannel#4&2f42c713&0&1#{2accfe60-c130-11d2-b082-
00a0c91efb8b}[deviceinstance]
   Oueries value:
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
84ae-d30803bae505}[default]
                                                            HKLM\system\currentcontrolset\control\deviceclasses\{2e34d650-5819-42ca-
   Queries value:
84ae-d30803bae505}\##?#root#vdrvroot#0000#{2e34d650-5819-42ca-84ae-d30803bae505}[deviceinstance]

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

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-1bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&1c83c2e&0&0001#{378de44c-56ef-11d1-bc8c-
OdaoC91405d4} [deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-56ef-11d1-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col02#6&1e20eb37&0&0001#{378de44c-56ef-11d1-bc8c
00a0c91405dd}[deviceinstance]
                                                            HKLM\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]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\\ 378de44c-56ef-11d1-bc8c-00a0c91405dd\\\##?\#hid\#vid_14dd\\\particlespid_1005\\ col03\#681e20eb37\\\ 080002\#\\\ 378de44c-56ef-11d1-bc8c-
00a0c91405dd}[deviceinstance]
```

DCSC-UU3UC914U50d3\##:#mldmvld_140dxpld_10U5&co1U3#6&1e2Ueb3/8U&UUU2#{3/8de44c-5bef-11d1-bc8c-00a0c91405dd}{deviceinstance} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{378de44c-5bef-11d1-bc8c-00a0c91405dd}\##?#root#rdp_mou#0000#{378de44c-5bef-11d1-bc8c-00a0c91405dd}\fdeviceinstance} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{11d1-bc8c-00a0c91405dd}\fdeviceinstance} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: AKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: AKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: AKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frac{1}{2} Queries value: AKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\fdeviceinstance\frace\frac{1}{2} Queries\frace\frace{1}{2} Queries\frace\frace{1}{2} Queries\frace\frace{1}{2} Queries\frace{1}{2} Qu

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27}\##?#pci#ven_8086&dev_27c9&subsys_01e61028&rev_01#3&2411e6fe&0&e9#{3abf6f2d-71c4-462a-8a92-1e6861e6af27}[deviceinstance]

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

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

94f2-00a0c91efb8b}\##?#scsi#disk8ven_dell&prod_virtual_disk#6&17b13437&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries \ value: \ HKLM\ system \ (current control set\ control\ device classes\ \{53f56307-b6bf-11d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#?\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\#6\&3af2ddc5\&0\&00000000\#\{53f56307-b6bf-14d0-94f2-00a0c91efb8b\}\ \#csi\#disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_disk\&ven\_dell\&prod\_virtual\_di
11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKl 94f2-00a0c91efb8b}[default]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
  Oueries value:
                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
t10n______#5&28836b8&0&0.0.0#{53f56308-b6bf-11d0-94f2-
Queries value: HKLM\system\cur
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
                                                       _1.0_
                                                                     #5&106af171&0&1.0.0#{53f56308-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                          HKLM\system\currentcontrolset\control\deviceclasses\{53f56308-b6bf-11d0-
  Oueries value:
94f2-00a0c91efb8b}\##?#ide#cdromvbox_cd-
                                                      ___1.0_____#5&394c0ad3&0&0.1.0#{53f56308-b6bf-11d0-94f2-
rom_
00a0c91efb8b}[deviceinstance]
                                            HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value: HKL 94f2-00a0c91efb8b}[default]
Queries value: HKLM\system\currentcontrolse
94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-
                                           HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
t10n_____1.02__#5&28836b88&0&0.0.0#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                          HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
  Oueries value:
00a0c91efb8b}[deviceinstance]

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

```
Oueries value:
                                                HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963}#0000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries \ value: \\ HKLM\system\currentcontrolset\control\deviceclasses\ \{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\}\ \ \#?\#storage\#volume\#\{74a4ebdb-f4e7-11df-aef6-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-defable-f4e8-de
806e6f6e6963}#0000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\{74a4ebdb-f4e7-11df-aef6-
806e6f6e6963\\\00000000000020f3026800\\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\\deviceipstance\
Queries value: HKLM\system\currentcontrol\set\control\
94f2-00a0c91efb8b\\##?#storage#volume#{74a4ebdb-f4e7-11df-aef6-
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
806e6f6e6963}#000000211262e800#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
   Oueries value:
94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-
806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
806e6f6e6963}#000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\{e29ac6c3-7037-11de-816d-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000000075343e0000#{5375630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000001e628b7200#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963}#0000020d3a1e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
806e6f6e6963}#00000020f3026800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\53f5630d-b6bf-11d0-94f2-00a0c91efb8b\\#;?#storage#volume#\{e29ac6c3-7037-11de-816d-
806e6f6e6963}#000000211262e800#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volume#{e29ac6c3-7037-11de-816d-
806e6f6e6963\}\#0000002131c36800\#\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b\}[deviceinstance]
                                               HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
   Oueries value:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot1#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
   Oueries value:
                                               HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b\} \verb||#|| *|#storage#volumesnapshot|| *|harddiskvolumesnapshot|| 10 # \{53f5630d-b6bf-11d0-94f2-b6bf-11d0-94f2-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d
00a0c91efb8b}[deviceinstance]
00a0c91efb8b}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot2#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
   Queries value:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot3#{53f5630d-b6bf-11d0-94f2
00a0c91efb8b}[deviceinstance]
                                               HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
   Oueries value:
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot4#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
   Oueries value
                                               HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot5#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]
00a0c91efb8b}[deviceinstance]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\##?#storage#yolumesnapshot#harddiskvolumesnapshot7#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b\} \verb||##?#storage|| wolumesnapshot|| where the storage for t
00a0c91efb8b}[deviceinstance]
   Oueries value:
                                               HKLM\svstem\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
Queries value.

94f2-00a0c91efb8b}\##?#storage#volumesnapshot#harddiskvolumesnapshot9#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
   Oueries value
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
94f2-00a0c91efb8b}[default]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{53f5630e-b6bf-11d0-
   Oueries value:
94f2-00a0c91efb8b}\##?#root#volmgr#0000#{53f5630e-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
85bb-30ff1f953599}[default]

Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype
Queries Value.

Ocryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]

Queries value:

HKLM\system\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e6102&&rev_02#4&1fc3087&0&2&f0#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]

Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\{5b45201d-f2f2-4f3b-
85bb-30ff1f953599}\##?#pci#ven_1002&dev_515e&subsys_01e61028&rev_02#4&2e5a831d&0&28f0#{5b45201d-
f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
                                               HKLM\svstem\currentcontrolset\control\deviceclasses\{5b45201d-f2f2-4f3b-
  Oueries value:
85bb-30ff1f953599}\##?#pci#ven_80ee&dev_beef&subsys_00000000&rev_00#3&267a616a&0&10#{5b45201d-f2f2-4f3b-85bb-30ff1f953599}[deviceinstance]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
843e-32c86e1ba19f}[default]
                                               HKLM\system\currentcontrolset\control\deviceclasses\{65a9a6cf-64cd-480b-
  Oueries value:
HKLM\system\currentcontrolset\control\deviceclasses\{72631e54-78a4-11d0-
   Queries value:
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-
   Oueries value:
a537-0000f8753ed1}[default]
                                                HKLM\system\currentcontrolset\control\deviceclasses\{811fc6a5-f728-11d0-
  Oueries value:
a537-0000f8753ed1}\##?#lptenum#microsoftrawport#5&98f833e&0&lpt1#{811fc6a5-f728-11d0-a537-
0000f8753ed1}[deviceinstance]
   Oueries value
                                                HKLM\system\currentcontrolset\control\deviceclasses\{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[default]
                                                HKI M\system\currentcontrolset\control\deviceclasses\{866519h5-3f07-4c97-
   Oueries value:
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#582dcf5eab80&12345678&06805#{866519b5-3f07-4c97-
b7df-24c5d8a8ccb8}[deviceinstance]
                                                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]

```
Oueries value:
                                                    HKLM\svstem\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
bc8c-00a0c91405dd}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
bc8c-00a0c91405dd}\##?#acpi#pnp0303#4&1d401fb5&0#{884b96c3-56ef-11d1-bc8c-
00a0c91405dd}[deviceinstance]
   Oueries value:
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1c83c2e&0&0000#{884b96c3-56ef-11d1-bc8c
00a0c91405dd}[deviceinstance]
                                                    HKI M\system\currentcontrolset\control\deviceclasses\{884b96c3-56ef-11d1-
 bc8c-00a0c91405dd}\##?#hid#vid_14dd&pid_1005&col01#6&1e20eb37&0&0000#{884b96c3-56ef-11d1-bc8c-
00a0c91405dd}[deviceinstance]
HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
   Oueries value:
af1f-0000f800845c}[default]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\deviceclasses\{97f76ef0-f883-11d0-
af1f-0000f800845c}\##?#acpi#pnp0400#4&1d401fb5&0#{97f76ef0-f883-11d0-af1f-
0000f800845c}[deviceinstance]
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
   Oueries value
359c-8bef029dbdd0}[default]
   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#_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_____
8bef029dbdd0}[deviceinstance]
                                                                __x3220__@_2.40ghz#_2#{97fadb10-4e33-40ae-359c-
Oueries value: HKLM\system\currentcontroiset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset\controlset
                                                  8bef029dbdd0}[deviceinstance]
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{97fadb10-4e33-40ae-
   Oueries value:
Spc-abefo29dbdd0}\##?#acpi#genuineintel___x86_family_6_model_15__
_intel(r)_xeon(r)_cpu____x3220__@_2.40ghz#_4#{97fadb10-4e33-40ae-359c-
8bef029dbdd0}[deviceinstance]
Queries value: HKI
901f-00c04fb951ed}[default]
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#usb#vid_14dd&pid_1005#bacc6f7f7e34a9bc#{a5dcbf10-6530-11d2-901f-
00c04fb951ed}[deviceinstance]
Queries value: HKLMsystem\currentcontrolset\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-
   Queries value:
8dcb-00c04fc3358c}[default]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0 8dcb-00c04fc3358c}\##?#pci#ven_14e4&dev_1659&subsys_01e61028&rev_11#4&188bd7e4&0&00e4#{ad498944-7659}
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
762f-11d0-8dcb-00c04fc3358c){deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c\} \\ \text{\#?\#pci\#ven\_14e4\&dev\_1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#4\&27c84f55\&0\&00e4\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#\{ad498944-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11\#\{ad49844-1659\&subsys\_01e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&rev\_11e61028\&r
 762f-11d0-8dcb-00c04fc3358c}[deviceinstance]
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Oueries value:
Queries value.

8dcb-00c04fc3358c}\##?#pci#wen_8086&dev_100e&subsys_001e8086&rev_02#3&267a616a&0&18#{ad498944-7621-11d0-8dcb-00c04fc3358c}[deviceinstance]
Queries \ value: HKLM \ system \ (current control \ device classes \ \{ad 498944-762f-11d0-8dcb-00c04fc3358c\} \ \ "renot* is a tap#0000\# \{ad 498944-762f-11d0-8dcb-00c04fc3358c\} \ \ [device in stance]
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Oueries value:
Queries Value: httm://www.ntcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcurrentcu
00c04fc3358c}[deviceinstance]
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Oueries value:
8dcb-00c04fc3358c}\##?#root#ms_12tpminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
   Oueries value
                                                  HKLM\svstem\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#ms_ndiswanbh#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
Oueries value: HKLM\system\currentcontrol\set\control\deviceclasses\{ad498944-762f-11d0-8dcb-00c04fc3358c}\#?#root#ms_ndiswanip#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
8dcb-00c04fc3358c}\##?#root#ms_ndiswanipv6#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Queries value:
8dcb-00c04fc3358c\} \verb|\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb|} = 0.00004fc3358c\} \verb|\##?#root#ms_pppoeminiport#0000#{ad498944-762f-11d0-8dcb|} = 0.00004fc3358c
00c04fc3358c}[deviceinstance]
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
   Oueries value:
8dcb-00c04fc3358c}\##?#root#ms_pptpminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\deviceclasses\{ad498944-762f-11d0-
 8dcb-00c04fc3358c}\##?#root#ms_sstpminiport#0000#{ad498944-762f-11d0-8dcb-
00c04fc3358c}[deviceinstance]
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:
82e6-71a87abac361}\##?#root#*isatap#0000#{cac88484-7515-4c03-82e6-71a87abac361}{[deviceinstance]}
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
8266-71a87ahac361}\##2#root#*teredo#0000#{cac88484-7515-4c03-82e6-71a87ahac361}[deviceinstance]
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_agilevpnminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_12tpminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
   Oueries value:
                                                   HKLM\svstem\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_ndiswanbh#0000#{cac88484-7515-4c03-82e6
71a87abac361}[deviceinstance]
   Oueries value:
                                                   HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 82e6-71a87abac361}\##?#root#ms_ndiswanip#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
    Queries value
                                                    HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
```

```
82e6-71a87abac361}\\##?#root#ms ndiswanipv6#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_pppoeminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
   Oueries value:
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
82e6-71a87abac361}\##?#root#ms_pptpminiport#0000#{cac88484-7515-4c03-82e6-
71a87abac361}[deviceinstance]
   Oueries value:
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{cac88484-7515-4c03-
 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-
bcaa-942b18988098}[default]
   Oueries value:
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
bcaa-942b18988098}\##?#usb#root_hub#4&152cc752&0#{ed8cf6b1-62d5-4597-bcaa-
942b18988098}[deviceinstance]
\label{lem:mass} Queries value: HKLM\system\currentcontrolset\control\deviceclasses\end{2.5} HKLM\system\currentcontrolset\control\deviceclasses\end{2.5} Additional engagement of the control deviceclasses $$ \end{2.5} Additional engagement of the contr
942b18988098}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\\{ed8cf6b1-62d5-4597-bcaa-942b18988098\\\#?\#usb\#root_hub\#482a2237a3\\00e408cf6b1-62d5-4597-bcaa-
942b18988098}[deviceinstance]
942b10360036}[uevleinstanke]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses
bcaa-942b18988098}\##?#usb#root_hub20#4&305beb5180#{ed8cf6b1-62d5-4597-bcaa-
                                                           HKLM\system\currentcontrolset\control\deviceclasses\{ed8cf6b1-62d5-4597-
00a0c906bed8}[deviceinstance]
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
    Queries value:
8815-00a0c906bed8}\##?#usb#root_hub#4&152cc752&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
   Oueries value:
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
8815-00a0c906bed8}\##?#usb#root_hub#4&22939226&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\\f18a0e88-c30c-11d0-8815-00a0c906bed8\\##?#usb#root_hub#4824693ec3&0#\f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrolset\control\deviceclass
8815-00a0c906bed8}\##?#usb#root_hub#4&2a2237a3&0#{f18a0e88-c30c-11d0-8815-
                                                           HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
00a0c906bed8}[deviceinstance]
                                                           HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
    Queries value:
8815-00a0c906bed8}\##?#usb#root_hub#4&395eaf14&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
                                                          HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
    Oueries value:
8815-00a0c906bed8}\##?#usb#root_hub20#4&211f73e0&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
    Oueries value
                                                         HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
 8815-00a0c906bed8}\##?#usb#root_hub20#4&305beb51&0#{f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Oueries value: HKLM\system\currentcontrolset\control\deviceclasses\\f18a0e88-c30c-11d0-
8815-00a0c906bed8\\##?#usb#vid_04b4&pid_6560#5&39c97729&0&3#\\f18a0e88-c30c-11d0-8815-
00a0c906bed8}[deviceinstance]
Queries value: HKLM\system\currentcontrol\set\control\deviceclasses\\f18a0e
8815-00a0c906bed8\\##?#usb#vid_04b4&pid_6560#5&b63c61a&0&3#\f18a0e88-c30c-11d0-8815-
                                                           HKLM\system\currentcontrolset\control\deviceclasses\{f18a0e88-c30c-11d0-
00a0c906bed8}[deviceinstance]
    Queries value:
HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[service]
HKLM\system\currentcontrolset\enum\umb\umb\1&841921d&0&printerbusenumerator[classguid]
    Queries value
                                                           HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
08002be10318}[lowerfilters]
    Oueries value
HKLM\system\currentcontrolset\enum\umb\1&841921d&0&printerbusenumerator[lowerfilters]
    Oueries value:
                                                           HKLM\svstem\currentcontrolset\services\umbus\enum[count]
                                                           HKLM\system\currentcontrolset\services\umbus\enum[0]
HKLM\system\currentcontrolset\services\umbus\enum[1]
     Queries value:
    Queries value:
    Queries value:
                                                           HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
    Oueries value:
Queries value: HKLM\system\currentcontrolset\enum\umb\\math\18841921d&0&printerbusenumerator[upperfilters]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e97d-e325-11ce-bfc1-
08002be10318}[upperfilters]

Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7[name]
Queries value: HKLM\software\microsoft\cry
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7[name]
                                                           HKLM\software\microsoft\cryptography\oid\encodingtype
Queries value: 
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
                                                           HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
    Oueries value:
    Oueries value:
\label{thm:hamiltonian} HKLMNsystem \current control set \services \prize \pr
nt\currentversion\compatibility32[spoolsv]
                                                           HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
                                                            HKLM\software\microsoft\windows\currentversion[devicepath]
    Oueries value:
Queries value:
8242-e03a18b5be01]
                                                            Oueries value:
                                                            HKLM\system\currentcontrolset\control\print[exceptionhandlerenabled]
                                                            HKLM\system\currentcontrolset\control\print[threadnotifymax]
                                                            HKLM\svstem\currentcontrolset\control\print[threadnotifvidlelife]
    Oueries value:
                                                            HKLM\system\currentcontrolset\control\print[threadmotifysleep]
HKLM\system\currentcontrolset\control\print[maxrpcsize]
    Queries value:
    Queries value:
                                                           HKLM\system\currentcontrolset\control\print[maxrpccalls]
HKLM\system\currentcontrolset\control\print[maxrpccalls]
HKLM\system\currentcontrolset\control\print[callexitprocesses[71e8376c]]
HKLM\system\currentcontrolset\control\print[callexitprocessonshutdown]
    Oueries value
    Queries value
    Oueries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]
    Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\tcpip\parameters[disableipsourcerouting] \\ Queries\ value: HKLM\system\currentcontrolset\services\tcpip\parameters[arpretrycount] \\
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\tcpip\parameters[igmplevel]
    Oueries value:
                                                            HKLM\system\currentcontrolset\services\tcpip\parameters[igmpversion]
    Queries value:
\label{lem:hklmsystem} HKL \\ \texttt{M\system} \\ \texttt{Current} \\ \texttt{Construct} \\ \texttt{Constr
```

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

```
HKLM\system\currentcontrolset\services\tcpip\parameters[disabletaskoffload]
 Oueries value
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledhcpmediasense]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable medias enseeventlog]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablemulticastforwarding]
HKLM\svstem\currentcontrolset\services\tcpip\parameters[enablepmtudiscovery]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpuserfc1122urgentpointer]
 Oueries value
\label{thm:control} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdataretransmissions] \end{tabular}
 Oueries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcptimedwaitdelay]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[tcpfinwait2delay]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtubhdetect]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcp1323opts]
 Oueries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters[enabletcpa]
 Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters[enabledca]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableconnectionratelimiting]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
 Queries value
\label{thm:hklm} HKLM\system\currentcontrolset\services\tcpip\parameters[qualifying destination threshold] \\ Queries\value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[ipautoconfigurationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationsubnet]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationmask]
 Oueries value:
                         HKLM\svstem\currentcontrolset\services\tcpip\parameters[ipenablerouter]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[arpuseethersnap]
  Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[overridedefaultaddressselection]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxuserport]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[ipaddress]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[subnetmask1
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[ipautoconfigurationaddress]
 Queries value:
c19ce8a73253}[ipautoconfigurationenabled]
 Oueries value:
c19ce8a73253}[performrouterdiscovery]
 Oueries value
c19ce8a73253}[defaultgateway]
 Queries value
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[defaultgatewaymetric]
c19ce8a73253}[solicitationaddressbcast]
 Queries value:
\label{local-parameters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253\}[usezerobroadcast]
 Oueries value:
\text{\text{WLMISystem\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[typeofinterface]
c19ce8a73253}[mtul
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[interfacemetric]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[tcpackfrequency]
 Queries value:
c19ce8a73253}[tcpdelackticks]
                         HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
 Oueries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
 Queries value:
Queries value:
                         HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a544a85b]
HKLM\software\microsoft\com3[finalizeractivitybypass]
 Oueries value:
                         HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\progid[]
                         HKCR\clsid\{e573ab3-1cc4-4404-bed3-ce037f170423}f]
HKCR\clsid\{e573ab5-1cc4-4404-bed3-de0991ff0623}[]
HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\progid[]
 Queries value:
 Oueries value:
                         HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}[]
HKLM\system\currentcontrolset\services\vss\settings[idletimeout]
 Queries value:
 Queries value:
 Oueries value:
                         HKLM\system\setup[upgradeinprogress]
HKLM\system\currentcontrolset\services\vss\settings[activewriterstatetimeout]
 Queries value:
Queries value:
                         HKLM\system\currentcontrolset\services\vss\diag[]
HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\progid[]
HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}[]
 Oueries value
 Queries value:
 Oueries value:
                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[]
 Oueries value
                         HKCR\clsid\{4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocse
                        /er32[threadingmodel]
                         HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
 Oueries value:
                         Queries value:
 Queries value:
 Oueries value
                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[]
                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[inprocserver32]
                         HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
 Queries value
```

```
HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\progid[]
  Oueries value:
                                                HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
HKCR\clsid\{7542e960-79c7-11d1-88f9-
   Queries value:
  Queries value:
0080c7d771bf}\inprocserver32[inprocserver32]
                                                HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
HKCR\clsid\{7542e960-79c7-11d1-88f9-
  Oueries value
0080c7d771bf}\inprocserver32[threadingmodel]
                                                HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
  Queries value:
                                                Oueries value:
   Queries value
  Oueries value:
                                                HKLM\system\currentcontrolset\services\wersyc\parameters[servicedll1]
   Queries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicemanifest]
  Queries value:
Queries value:
                                                a440-f1f52d28711d1
  Queries value:
                                                HKLM\software\microsoft\windows\windows error reporting[servicetimeout]
   Queries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicedllunloadonstop]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[imgsvc]
  Oueries value:
                                                HKLM\svstem\currentcontrolset\services\stisvc\parameters[servicedll]
   Queries value:
HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest]
  Queries value:
Queries value:
                                                {\tt HKLM \ } system \verb| current control set \verb| services \verb| stisvc \verb| parameters [service main]|
Queries value:
   Queries value:
Oueries value:
HKLM \verb|\system| current controls et \verb|\control| stillimage \verb|\trace[default tracelevel]|
   Queries value:
\label{thm:hkkm} HKLM \noindent \n
Oueries value
HKLMIsystem \current controls et \control still image \trace \wiaservc. dll[traceflags] \\ Queries value:
HKLM\svstem\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracemask]
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracelevel]
   Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[maxtracearraysize]
  Oueries value
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[enableobjecttracking]
  Oueries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dl1[heapoptions]
Queries value: HKLM\software\microsoft\rpc\securityservice[10]
                                                HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}{authenticationlevel1
   Oueries value:
   Queries value:
                                                 HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[accesspermission]
                                                HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\progid[]
  Oueries value:
                                                HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[]

HKLM\software\microsoft\sqmclient\windows\disabledprocesses[34dba8a7]

HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}[]
   Queries value:
  Queries value:
  Oueries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\stillimage[deviceid]
   Oueries value:
HKLMNsystem\currentcontrolset\control\stillimage\events\connected[defaulthandler]

Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected[guid]
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\connected\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[name]
   Queries value
HKLM\system\currentcontrolset\control\stillimage\events\connected\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[desc1
\label{limage-events-connected-438f8a702-36bb-4a68-80e6-d4966b9bb718} [icon] \\
  Queries value:
\label{limage-events-connected-438f8a702-36bb-4a68-80e6-d4966b9b718} [cmdline] \\
  Oueries value:
\label{lem:hklm} \verb+KkLM\+ system \land current control \verb+stillimage \land events \land disconnected \texttt{[defaulthandler]} + \texttt{the lem system} \land disconnected \texttt{[defaulthandler]} + \texttt{the lem
  Queries value:
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage[defaulthandler]
                                                HKLM\system\currentcontrolset\control\stillimage\events\emailimage[guid]
  Queries value:
759eb35cdf9a}[name]
  Oueries 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:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[cmdline]
  Queries value:
\label{limited} HKLM\system\currentcontrolset\control\stillimage\events\faximage\[defaulthandler\] \\ Queries\ value: HKLM\system\currentcontrol\stillimage\events\faximage\[guid\] \\
  Oueries value:
Oueries value
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[desc]
Queries value: 
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
  Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[cmdline]
  Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage[defaulthandler]
Queries value: HKLM\system\currentcontrol\stillimage\events\printimage[guid]
   Oueries value:
```

HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-

O0cO4fb926af}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]

 $\label{eq:hkcr_interface} HKCR\interface \\ \{00000100-0000-0000-0000-000000000046\}\proxystubclsid32[]\\ HKCR\interface\\ \{609b9555-4fb6-11d1-9971-00c04fbb345\}\proxystubclsid32[]\\ HKCR\interface\\ \{609b9555-4fb6-11d1-9971-00c04fbb345]\proxystubclsid32[]\\ HKCR\interface\\ \{609b9555-4fb6-11d1-9971-00c04fb5-11d1-9971-00c04fb5-11d1-9971-00c04fb5-11d1$

Oueries value:

Queries value: Queries value:

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

Queries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[guid]
  Oueries value
\text{Vectors value.} 
   Queries value
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[desc]
  Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-
d4966b9bb718}[icon]
  Queries value:
\label{limage-events-scan} HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{38f8a702-36bb-4a68-80e6-d4966b9bb718}[cmdline]
  Oueries value
HKLMNsystem \current control set \control \stillimage \events \scan but ton \{5f4baad0-4d59-4fcd-b213-783ce7a92f22\} [name] \\
783ce7a92f22}[desc]
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}[cmdline]
  Queries value:
\label{limage} HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}\ [name]
  Oueries value:
759eb35cdf9a}[desc1
Queries value: 
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[icon]
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}[name]
  Oueries value:
HKLMNsystem \current control set \control \still image \events \scan but ton \eabbd 70d-a25f-4e90-96a4-7105fd3b53b1 \end{substitute} [desc]
  Oueries value
\label{thm:control} HKLM \system \current control still image \events \scan but ton \eabbd 70d-a 25f-4e 90-96a 4-but to \end{area}.
7105fd3b53b1}[icon]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}[cmdline]
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[defaulthandler]
   Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[guid]
   Oueries value
HKLM\system\currentcontrolset\control\stillimage\serversettings[shutdownifunuseddelay]
  Oueries value:
                                       HKLM\system\currentcontrolset\services\nativewifip[imagepath]
                                       HKLMN.systemNcurrentcontrolset\services\nativewifip[lmagepatn]
HKLMN.systemNcurrentcontrolset\services\nativewifip[objectname]
HKLMNsystemNcurrentcontrolset\services\nativewifip[type]
HKLMN.systemNcurrentcontrolset\services\nativewifip\enuf]
HKLMN.systemNcurrentcontrolset\services\nativewifip\enuf]
HKLMN.systemNcurrentcontrolset\enum\root\legacy_nativewifip\0000[service]
   Queries value:
  Queries value:
   Oueries value:
   Queries value:
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[classguid]
   Oueries value
                                       HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-
0000f8753ed1}[lowerfilters]
  Oueries value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[lowerfilters]
  Queries value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[upperfilters]
Queries value: HKLM\system\currentcontrolset\control\class\{8ecc055d-047f-11d1-a537-
0000f8753ed1}[upperfilters]
   Queries value:
                                       HKLM\system\currentcontrolset\services\nativewifip[pnpflags]
  Queries value:
99ea-fe66a8355df8]
Queries value:
                                        Queries Value: hKLM\system\currentcontrol\set\control\network\\\ 4d36e974-e325-11ce-bfc1-
08002be10318}\\\ e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filtertype]
Queries value: HKLM\system\currentcontrol\set\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]
  Oueries value
Oueries value:
                                       HKLM\system\currentcontrolset\enum\root\ms ndiswanipv6\0000[driver]
Queries value: HKLM\system\
08002be10318}\0005\linkage[upperbind]
                                        Oueries value:
                                        HKLM\svstem\currentcontrolset\enum\root\ms ndiswanip\0000[driver]
                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\linkage[upperbind]
                                       HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
  Queries value
08002be10318}\0006\linkage[upperbind]
   Queries value:
HKLM\system\currentcontrolset\enum\pci\ven 8086&dev 100e&subsys 001e8086&rev 02\3&267a616a&0&18[driver]
Queries value: HKLM\system\
08002be10318\\0007\linkage[upperbind]
                                        HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Oueries value:
                                        HKLM\svstem\currentcontrolset\services\ndisuio[imagepath]
   Queries value:
                                        HKLM\system\currentcontrolset\services\ndisuio[objectname]
  Oueries value:
                                        HKLM\system\currentcontrolset\services\ndisuio[type]
                                       HKLM\system\currentcontrolset\services\ndisuio\enum[count]
HKLM\system\currentcontrolset\services\ndisuio[displayname]
   Queries value:
   Queries value:
                                       HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[classguid]
   Oueries value:
   Queries value:
   Oueries value:
```

HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[lowerfilters]

```
Oueries value
\label{local_holds} \begin{tabular}{ll} HKLM \end{tabular} which is a partial control of the local control of th
                                                           HKLM\system\currentcontrolset\services\ndisuio[pnpflags]
    Queries value:
    Oueries value
                                                           HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-
 aded-5304bf8f636d]
    Oueries value
                                                           HKLM\system\currentcontrolset\control\wmi\securitv[b3eee223-d0a9-40cd-
adfc-50f1888138ab]
    Queries value:
                                                           HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[driver]
Oueries value
                                                           HKLM\system\currentcontrolset\enum\root\ms pptpminiport\0000[driver]
Queries value: HKLM\system\
08002be10318}\0003\linkage[upperbind]
                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
                                                          HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Oueries value
    Queries value
08002be10318}\0004\linkage[upperbind]
    Queries value
                                                           HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[driver]
                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Queries value
08002be10318}\0002\linkage[upperbind]

Queries value: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
    Oueries value
                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\linkage[upperbind]
                                                           HKLM\system\currentcontrolset\enum\root\*teredo\0000[driver]
    Queries value:
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\linkage[upperbind]
    Oueries value:
                                                           HKLM\svstem\currentcontrolset\enum\root\*isatap\0000[driver]
Queries value: HKLM\system\
08002be10318}\0009\linkage[upperbind]
                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Oueries value
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
   Oueries value:
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[start]
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
   Queries value
context logger[flushthreshold]
   Queries value: HKLM\:
                                                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[buffersize]
    Queries value
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[minimumbuffers]
    Queries value:
                                                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[flushtimer]
   Oueries value
                                                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maximumbuffers]
                                                          HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
   Oueries value
context logger[filename]
                                                           {\tt HKLM \control \c
   Queries value
context logger[enablekernelflags]
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
    Queries value
context logger[stackwalkingfilter]
    Queries value:
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[clocktype]
   Oueries value
                                                          HKLM\svstem\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maxfilesize]
   Oueries value
                                                          HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[logfilemode]
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
   Queries value
context logger[disablerealtimepersistence]
Queries value: HKLM\system\curren
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[guid]
    Queries value
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filecounter]
    Oueries value
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filemax]
   Oueries value
                                                           HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
Context logger[pooltagfilter]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-
af71-3e63d056f1741
    Sets/Creates value:
                                                           HKLM\system\currentcontrolset\enum\root\legacy_nativewifip[nextinstance]
    Sets/Creates value
HKLM\system\currentc
                                                         olset\enum\root\legacy_nativewifip\0000\control[*newlycreated*
                                                           HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[service]
    Sets/Creates value:
    Sets/Creates value
                                                           Sets/Creates value
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[configflags]
    Sets/Creates value
                                                           HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[class]
    Sets/Creates value
\label{thm:loss} HKLM\system\currentcontrolset\enum\root\legacy\_native wifip\0000[classguid] \\ Sets/Creates\ value:
HKLM\system\currentcontrolset\enum\root\legacy_nativewifip\0000[devicedesc]
    Sets/Creates value:
                                                           HKLM\system\currentcontrolset\services\nativewifip\enum[0]
                                                           HKLM\system\currentcontrolset\services\nativewifip\enum[count]
    Sets/Creates value
    Sets/Creates value
                                                           HKLM \verb|\system| current controlset \verb|\services| native wifip \verb|\enum[nextinstance]|
     Sets/Creates value
Sets/Creates value
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
    Sets/Creates value:
Sets/Creates value:
                                                          HKLM\system\currentcontrolset\services\nativewifip[ndismajorversion] HKLM\system\currentcontrolset\services\nativewifip[ndisminorversion]
    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
                                                           HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[service]
HKLM\system\currentcontrolset\enum\root\legacy_ndisuio\0000[legacy]
    Sets/Creates value
     Sets/Creates value
                                                          \label{thm:loss} HKLM \system \current controls et \enum \noot \legacy_n disuio \noot \cite{loss} HKLM \system \current \cot \cite{loss} class \cite{loss} loss \cite{loss} lo
    Sets/Creates value
    Sets/Creates value
                                                          \label{thm:loss} HKLM\system\currentcontrolset\enum\root\legacy\_ndisuio\00000[classguid] \\ HKLM\system\currentcontrolset\enum\root\legacy\_ndisuio\00000[devicedesc] \\ HKLM\system\currentcontrolset\services\ndisuio\enum[0]
    Sets/Creates value
    Sets/Creates value
    Sets/Creates value
    Sets/Creates value
                                                           HKLM\svstem\currentcontrolset\services\ndisuio\enum[count]
    Sets/Creates value
                                                           HKLM\system\currentcontrolset\services\ndisuio\enum[nextinstance]
    Sets/Creates value
HKLM\system\currentcont
                                                        rolset\enum\root\legacy_ndisuio\0000\control[activeservice]
HKLM\system\currentcontrolset\services\ndisuio[ndismajorversion]
    Sets/Creates value
                                                          \label{thm:hklm} HKLM \system \current control set \current control set \current control set \current control \current control \current 
    Sets/Creates value
     Value changes:
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-32c86e1ba19f}\##?#umb#umb#1&841921d&0&printerbusenumerator#{65a9a6cf-64cd-480b-843e-
 32c86e1ba19f}\control[referencecount]
                                                           HKLM\system\currentcontrolset\services\umbus\enum[count]
    Value changes:
    Value changes:
                                                           HKLM\system\currentcontrolset\services\umbus\enum[nextinstance]
    Value changes:
                                                           HKLM\system\currentcontrolset\services\nativewifip\enum[count]
    Value changes:
                                                          HKLM\system\currentcontrolset\services\nativewifip\enum[nextinstance] HKLM\system\currentcontrolset\services\ndisuio\enum[count]
     Value changes
    Value changes:
                                                           HKLM\svstem\currentcontrolset\services\ndisuio\enum[nextinstance]
```

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

Value changes

context logger[status]