# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3319, Task ID: 786

Task ID: 786 Risk Level: 10

Date Processed: 2016-05-18 10:38:07 (UTC)

Processing Time: 28.56 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe"

Sample ID: Type: basic Owner: admin

f0d96afe8a3c58bf99f8b24ff10b1a07 Label: 2016-05-18 10:30:50 (UTC)

Date Added: PE32:win32:gui

File Type: File Size: 93184 bytes

f0d96afe8a3c58bf99f8b24ff10b1a07 MD5:

d04b163e862ba9ead5cf9f379edf96bde8a146b4aea6987312b2a739c0b81701 SHA256:

Description: None

### Pattern Matching Results

10 Creates malicious events: Beebone [Trojan]

4 Terminates process under Windows subfolder

3 Long sleep detected

6 Checks task list from command line

#### Static Events

Anomaly: PE: Contains a virtual section

### Process/Thread Events

C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe Creates process:

["C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe" ]

C:\Windows\SysWOW64\cmd.exe ["C:\Windows\System32\cmd.exe" /c Creates process:

tasklist&&del f0d96afe8a3c58bf99f8b24ff10b1a07.exe]

Creates process: C:\Windows\SysWOW64\tasklist.exe [tasklist]

Terminates process: C:\Windows\Temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe

Terminates process: C:\Windows\SysWOW64\tasklist.exe Terminates process: C:\Windows\SysWOW64\cmd.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex Creates mutex: \Sessions\1\BaseNamedObjects\\_!MSFTHISTORY!\_

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet

files!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies! Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

\Sessions\1\BaseNamedObjects\WininetStartupMutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex Creates mutex:

\Sessions\1\BaseNamedObjects\RasPbFile Creates mutex:

\Sessions\1\BaseNamedObjects\ZonesCounterMutex Creates mutex:

\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex:

\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex \Sessions\1\BaseNamedObjects\!IETld!Mutex Creates mutex:

\KernelObjects\MaximumCommitCondition Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX Creates event: \BaseNamedObjects\ConsoleEvent-0x0000000000000950 Creates event:

\BaseNamedObjects\TermSrvReadyEvent Creates event:

\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP? Creates semaphore:

F0D96AFE8A3C58BF99F8B24FF10B1A07.EXE

## File System Events

Creates

Creates: C:\Users\Admin\AppData\Local

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files Creates:

C:\Users\Admin\AppData\Roaming Creates:

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies Creates:  ${\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\History}$ Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches Creates: C:\Windows\Prefetch\F0D96AFE8A3C58BF99F8B24FF10B1-664BA9E9.pf Opens:

Opens: C:\Windows

```
C:\Windows\System32\wow64.dll
 Opens:
                         C:\Windows\System32\wow64win.dll
 Opens:
 Opens:
                         C:\Windows\System32\wow64cpu.dll
 Opens:
                         C:\Windows\system32\wow64log.dll
 Opens:
                         C:\Windows\SysWOW64
                         C:\windows\temp\MSVBVM60.DLL
 Opens:
                         C:\Windows\SysWOW64\msvbvm60.dll
 Opens:
                         C:\Windows\SysWOW64\sechost.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\SysWOW64\rpcss.dll
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe.cfg
 Opens:
                         C:\windows\temp\SXS.DLL
 Opens:
                         C:\Windows\SysWOW64\sxs.dll
 Opens:
                         C:\Windows\System32\C_932.NLS
 Opens:
                         C:\Windows\System32\C_949.NLS
 Opens:
                         C:\Windows\System32\C_950.NLS
 Opens:
                         C:\Windows\System32\C_936.NLS
                         C: \verb|\windows\Temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe|
 Opens:
 Opens:
                         C:\
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
                         C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe.Local\
 Opens:
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
                         C:\windows\temp\profapi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
 Opens:
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\index.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
                         C:\windows\temp\dnsapi.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\windows\temp\iphlpapi.DLL
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\windows\temp\WINNSI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\windows\temp\RASAPI32.dll
                         C:\Windows\SysWOW64\rasapi32.dll
 Opens:
 Opens:
                         C:\windows\temp\rasman.dll
 Opens:
                         C:\Windows\SysWOW64\rasman.dll
 Opens:
                         C:\windows\temp\rtutils.dll
 Opens:
                         C:\Windows\SysWOW64\rtutils.dll
 Opens:
                         C:\ProgramData\Microsoft\Network\Connections\Pbk\
                         C:\Windows\SysWOW64\ras
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\windows\temp\sensapi.dll
                         C:\Windows\SysWOW64\SensApi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\nlaapi.dll
 Opens:
                         C:\windows\temp\rasadhlp.dll
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
 Opens:
                         C:\windows\temp\ntmarta.dll
                         C:\Windows\SysWOW64\ntmarta.dll
 Opens:
 Opens:
                         C:\windows\temp\VERSION.dll
 Opens:
                         C:\Windows\SysWOW64\version.dll
                         C:\Windows\SysWOW64\en-US\urlmon.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
                         C:\Windows\SysWOW64\wship6.dll
 Opens:
                         C:\windows\temp\dhcpcsvc6.DLL
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
                         C:\windows\temp\dhcpcsvc.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc.dll
```

Opens: C:\Windows\System32\drivers\etc\hosts

C:\windows\temp\PROPSYS.dll Opens: C:\Windows\SysWOW64\propsys.dll Opens: Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\windows\temp\apphelp.dll Opens: C:\Windows\SysWOW64\apphelp.dll C:\Windows\SysWOW64\ieframe.dll Opens: C:\Windows\SysWOW64\oleacc.dll Opens: Opens: C:\windows\temp\OLEACCRC.DLL Opens: C:\Windows\SysWOW64\oleaccrc.dll

Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-

4C77-AF34-C647E37CA0D9}.1.ver0x00000000000001.db

Opens: C:\Users\Admin\Desktop\desktop.ini
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Windows\Sys\0W64\en-US\propsys.dll.mui
Opens: C:\Windows\Sys\0W64\cmd.exe

Opens: C:\Windows\SysWOW64\cmd.exe:Zone.Identifier

Opens: C:\Windows\WINHELP.INI
Opens: C:\Windows\SysWOW64\.HLP
Opens: C:\Windows\Help\.HLP

Opens: C:\Windows\Prefetch\TASKLIST.EXE-178413B7.pf

Opens: C:\Windows\SysWOW64\mpr.dll Opens: C:\Windows\SysWOW64\secur32.dll Opens: C:\Windows\SysWOW64\framedynos.dll Opens: C:\Windows\SysWOW64\wtsapi32.dll Opens: C:\Windows\SysWOW64\netapi32.dll Opens: C:\Windows\SysWOW64\netutils.dll Opens: C:\Windows\SysWOW64\srvcli.dll Opens: C:\Windows\SysWOW64\wkscli.dll Opens: C:\Windows\SysWOW64\dbghelp.dll

Opens: C:\Windows\SysWOW64\en-US\tasklist.exe.mui Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui C:\Windows\SysWOW64\wbem\wbemprox.dll Opens: Opens: C:\Windows\SysWOW64\wbem\wbemcomn.dll Opens: C:\Windows\SysWOW64\wbemcomn.dll C:\Windows\SysWOW64\wbem\Logs Opens: Opens: C:\Windows\SysWOW64\winsta.dll Opens: C:\Windows\SysWOW64\cryptsp.dll C:\Windows\SysWOW64\rsaenh.dll Opens: Opens: C:\Windows\SysWOW64\RpcRtRemote.dll Opens: C:\Windows\SysWOW64\wbem\wbemsvc.dll  ${\tt C:\Windows\SysWOW64\wbem\fastprox.dll}\\$ Opens: Opens: C:\Windows\SysWOW64\wbem\NTDSAPI.dll Opens: C:\Windows\SysWOW64\ntdsapi.dll

Opens: C:\Windows\SysWOW64\wbem\en-US\wmiutils.dll.mui

 $\label{lem:condition} Opens: C:\windows\sysWOW64\f0d96afe8a3c58bf99f8b24ff10b1a07.exe \\ Reads from: C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe \\$ 

C:\Windows\SysWOW64\wbem\wmiutils.dll

Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Windows\Sys\WO\W64\cmd.exe
Reads from: C:\Windows\Sys\WO\W64\tasklist.exe

#### Network Events

DNS query: domai.05dns.biz
Sends data to: 8.8.8.8:53
Receives data from: 8.8.8.8:53

### Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings

Creates key: HKLM\software\wow6432node\microsoft\tracing

Creates key:

Opens:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus f0d96 afe8a3c58bf99f8b24ff10b1a07\_rasapi32$ 

Creates key:

settings\connections

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

Creates key: HKCU\software\microsoft\visual basic\6.0

Creates key: HKCU\software

Creates key: HKCU\software\microsoft

Creates key: HKCU\software\microsoft\visual basic

Creates key: HKLM\software\wow6432node\microsoft\wbem\cimom

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[autoconfigurl]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

Opens key:  ${\tt HKLM \setminus software \setminus microsoft \setminus windows\ nt \setminus current version \setminus image\ file\ execution}$ 

options

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

Opens key: HKLM\system\currentcontrol\set\control\terminal server
Opens key: HKLM\system\currentcontrol\safeboot\option
Opens key: HKLM\system\currentcontrol\set\control\srp\gp\dll

Opens key:

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrol\set\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

 $Opens\ key: \\ HKLM \ system \ current control set \ control \ mui \ uilanguages \ pending delete$ 

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

 $Opens~key: \\ HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside$ 

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre\_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

Opens key: HKLM\software\wow6432node\microsoft\ole

Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing

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

Opens key: HKLM\software\wow6432node\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key: HKLM\system\currentcontrol\set\control\nls\codepage
Opens key: HKLM\software\wow6432node\microsoft\vba\monitors

Opens key: HKCU\software\classes\
Opens key: HKLM\software\microsoft\com3

Opens key: HKCU\software\classes\wow6432node\clsid\{1857ee93-c29a-4421-bf5e-

4aff9abf109c}

Opens key: HKCR\wow6432node\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}
Opens key: HKCU\software\classes\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}

Opens key: HKCR\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}

Opens key: HKCU\software\classes\wow6432node\clsid\{2433df16-b661-424b-8b68-

94b7c9a8936e}

Opens key: HKCR\wow6432node\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e}
Opens key: HKCU\software\classes\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e}

Opens key: HKCR\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e} Opens key: HKLM\system\currentcontrolset\services\disk\enum

Opens key: HKLM\software\wow6432node\microsoft\rpc

Opens key: HKLM\system\currentcontrol\computername\activecomputername

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\services\crypt32

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer

Opens key: HKLM\software\policies\microsoft\internet explorer

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main

 $\label{lem:condition} Opens~key: $$ HKLM\software\policies\microsoft\internet explorer\main Opens~key: $$ HKLM\software\wow6432node\policies\microsoft\internet $$$ 

explorer\main\featurecontrol

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol

Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\content

Opens key:

 $\label{thm:hammon} \parbox{$HKLM} software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \parbox{$HKLM} \end{tabular} \parbox{$HKLM} \parbox{$MKLM} \parbox{$MKLM}$ 

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caed \ folder \ descriptions \ folder \ folder \ descriptions \ folder \ descriptions \ folder \ folder \ descriptions \ folder \ descriptions \ folder \ descriptions \ folder \ descriptions \ folder \$ 

Opens key

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$ 

Opens key: HKCU\software\microsoft\windows\currentversion\explorer

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer

Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer

Opens key:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1532785-65ba-4fcf-9d55-7b8e7f157091\}$ 

Opens key:

 $\label{thm:local-state} HKLM \software \wow 6432 node \verb|microsoft| windows \verb|currentversion| explorer \\folder descriptions \\folder de$ 

Opens key:

 $\label{thm:local-continuous} HKLM \software \wow6432 node \mbox{$ 5e6c858f-0e22-4760-9afe-ea3317b67173} \\$ 

Opens key

 $\label{thm:local-continuous} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173}\property bag$ 

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001

Opens kev:

Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies

Opens key:

 $\label{thm:local-prop} HKL\dot{M}\software\\\wow6432\\\node\\\microsoft\\\windows\\\currentversion\\\explorer\\\folderdescriptions\\\fo$ 

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16444, 2b0f765d-16444, 2b0f766d-16444, 2b0f766d-16444, 2b0f766d-16444, 2b0f76d-16444, 2b0f76d-164444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-164444, 2b0f7$ 

```
c0e9-4171-908e-08a611b84ff6}\propertybag
  Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}
  Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\history
                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\history
  Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d12b, d12b, d24b, d
b784-432e-a781-5a1130a75963}
  Opens key:
b784-432e-a781-5a1130a75963}\propertybag
  Opens key:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\domstore
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\feedplat
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\iecompat
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\ietld
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\privacie:
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
  Opens key:
                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                  HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                                  HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
                                  HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens kev:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                                  HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
  Opens kev:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
```

explorer\main\featurecontrol\feature\_digest\_no\_extras\_in\_uri

```
HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                  HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens kev:
                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature release keys on unload kb975619
 Opens key:
                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                  HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                  HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
                  HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\0262b795
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens kev:
Opens kev:
Opens key:
Opens key:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
                  HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens key:
 Opens key:
                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                  HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature http username password disable
 Opens key:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
 Opens kev:
HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07_rasapi32
 Opens kev:
Opens key:
                  HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key:
                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
 Opens key:
                   HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
```

```
Opens key:
                                   HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:
                                   HKU\
                                   Opens kev:
                                   HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens key:
  Opens key:
                                   HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:
                                   HKLM\system\currentcontrolset\services\dns
                                   HKLM\software\wow6432node\policies\microsoft\windows
  Opens key:
nt\dnsclient\dnspolicyconfig
                                   HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                   HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\domains
  Opens key:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\zonemap\ranges\
  Opens key:
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\ranges\
  Opens key:
                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                   HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                   HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_zones\_check\_zonemap\_policy\_kb941001
  Opens key:
HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap
                                   Opens key:
settings\zonemap
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\protocoldefaults\
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                   settings\zonemap\domains\
                                   HKLM\software\policies\microsoft\internet explorer\security
  Opens kev:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                   \label{lem:hkcu} \mbox{\current} windows \mbox{\current} internet settings \mbox{\current} settings \mbox{\current} and \mbox{\current} settings \mbox{\current} settings
  Opens kev:
                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones
  Opens key:
                                   settings\zones\
  Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ zones \ \ 0
  Opens key:
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:
                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:
```

```
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
 Opens kev:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
 Opens key:
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\zones\2
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                          HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer \verb|\main\featurecontrol\feature\_localmachine\_lockdown|
 Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet
settings\lockdown_zones\
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
settings\lockdown zones\0
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\1
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\lockdown zones\2
 Opens key:
settings\lockdown_zones\2
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
 Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\3
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
 Opens key:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\lockdown_zones\4
 Opens key:
settings\lockdown zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                          \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens kev:
settings\lockdown_zones\4
```

```
Opens key:
                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:
                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                             HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:
                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:
                             HKLM\system\currentcontrolset\control\lsa\accessproviders
  Opens key:
                             HKLM\system\currentcontrolset\services\ldap
                             HKCU\software\microsoft\internet explorer\ietld
  Opens key:
  Opens key:
                             HKLM\system\currentcontrolset\control\cmf\config
  Opens key:
                             HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:
                             HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:
                             HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:
                             HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens kev:
                             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:
                             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:
                             HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:
                             HKLM\software\policies\microsoft\system\dnsclient
                             HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
  Opens kev:
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
  Opens key:
                             HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
e1e01c1f69b5}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
  Opens key:
806e6f6e6963}
 Opens kev:
127795cce47a}
  Opens key:
65fee5bae0b1}
  Opens kev:
                             HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
                             HKLM\system\currentcontrolset\services\netbt\linkage
  Opens kev:
Opens key:
                             HKLM\software\wow6432node\microsoft\windows\currentversion\explorer
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key:
                             HKLM\software\microsoft\windows\currentversion\policies\explorer
                             HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens kev:
  Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ delegate folders
  Opens key:
Opens key:
7b94-4dc3-b131-e946b44c8dd5}
  Opens kev:
d933-450a-90e6-4acd2e9408fe}
  Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ name space \ \{11016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610
e366-4d22-bc06-4ada335c892b}
  Opens key:
a00a-44d7-9371-beb064c98683}
  Opens key:
038b-4685-ab02-99bb52d3fb8b}
  Opens key:
ad25-11d0-98a8-0800361b1103}
  Opens key:
6ce5-4d6c-8fce-1d8870fdcba0}
  Opens key:
3f72-44a7-89c5-5595fe6b30ee}
  Opens key:
5081-101b-9f08-00aa002f954e}
```

Opens key:

```
6bd1-4c86-9454-beb04e94c819}
      Opens key:
1c37-4a49-a12e-4b2d810d956b}
c1ea-428d-a78a-d1f5659cba93}
      Opens key:
21cb-41b2-a086-b309680c6b7e}
      Opens key:
e44d-46af-be1b-cbacea2c3065}
      Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{e345f35f-e16464, e16464, e16464
9397-435c-8f95-4e922c26259e}
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ namespace \ \{ed 228fdf-desktop \ namespace \ ed 228fdf-deskto
9ea8-4870-83b1-96b02cfe0d52}
be21-4350-88b0-7367fc96ef3c}
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ delegate folders
      Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows \ top \ names pace \ delegate folders
                                                                                              HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
      Opens key:
08002b30309d}\shellfolder
      Opens key:
                                                                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
                                                                                              HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta + (20d04fe0-delta + (20d0
      Opens key:
3aea-1069-a2d8-08002b30309d}\shellfolder
      Opens key:
a2d8-08002b30309d}\shellfolder
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\policies\nonenum
      Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
      Opens key:
                                                                                              HKLM\software\microsoft\windows\currentversion\policies\nonenum
                                                                                              HKCU\software\classes\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
      Opens kev:
08002b30309d}\shellfolder
                                                                                              Opens key:
 08002b30309d}\shellfolder
                                                                                              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{208d2c60-
      Opens key:
 3aea-1069-a2d7-08002b30309d}\shellfolder
      Opens kev:
a2d7-08002b30309d}\shellfolder
      Opens key:
                                                                                              HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-
08002b30309d}\shellfolder
      Opens key:
                                                                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 08002b30309d}\shellfolder
                                                                                              HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{871c5380-microsoft\} \ description 
      Opens key:
42a0-1069-a2ea-08002b30309d}\shellfolder
                                                                                              HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
      Opens key:
 08002b30309d}\inprocserver32
      Opens key:
                                                                                             HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 08002b30309d}\inprocserver32
                                                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\shell
      Opens kev:
 extensions\blocked
                                                                                              HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
      Opens kev:
      Opens key:
                                                                                              HKLM\system\currentcontrolset\control\session manager\appcompatibility
      Opens key:
                                                                                              HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| appcompat
      Opens key:
                                                                                              HKLM\software\policies\microsoft\windows\appcompat
      Opens kev:
                                                                                              HKCU\software\microsoft\windows nt\currentversion
      Opens key:
                                                                                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
                                                                                              HKLM\software\wow6432node\microsoft\windows
      Opens key:
nt\currentversion\appcompatflags
      Opens key:
                                                                                              HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\appcompatflags\custom\ieframe.dll
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\shell extensions\cached
      Opens key:
                                                                                              HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 08002b30309d}
                                                                                              HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
      Opens kev:
      Opens key:
                                                                                              HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-
 08002b30309d}\treatas
```

```
08002b30309d}\progid
                                                                                                                                            HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
          Opens key:
          Opens key:
                                                                                                                                            HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
                                                                                                                                            HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
          Opens key:
          Opens kev:
                                                                                                                                            HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
  08002b30309d}\progid
          Opens key:
                                                                                                                                            HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
          Opens key:
 08002b30309d}\inprochandler32
                                                                                                                                            HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
          Opens key:
 08002b30309d}\inprochandler32
          Opens key:
                                                                                                                                           HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-
  08002b30309d}\inprochandler
                                                                                                                                          HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
         Opens key:
 08002b30309d}\inprochandler
          Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibilitv\objects\{871c5380-
 42a0-1069-a2ea-08002b30309d}
                                                                                                                                           HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{645ff 040 - 5081 - 101b - 9f08 - 101b - 101
         Opens key:
 00aa002f954e}\shellfolder
                                                                                                                                           HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
          Opens key:
 00aa002f954e}\shellfolder
                                                                                                                                           Opens kev:
  5081-101b-9f08-00aa002f954e}\shellfolder
         Opens key:
 9f08-00aa002f954e}\shellfolder
                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
          Opens key:
 beb064c98683}\shellfolder
                                                                                                                                           HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
          Opens key:
 beb064c98683}\shellfolder
                                                                                                                                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \closer{lem:hkcu} \end{tabular} $$ Akcular \clsid \closer{lem:hkcular} \end{tabular} $$ Akcular \clsid \
         Opens key:
  a00a-44d7-9371-beb064c98683}\shellfolder
         Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (26ee 0668-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7
 9371-beb064c98683}\shellfolder
                                                                                                                                           HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
        Opens kev:
  5595fe6b30ee}\shellfolder
                                                                                                                                            HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
          Opens key:
 5595fe6b30ee}\shellfolder
                                                                                                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (59031a47-1) + (59031a47-
          Opens key:
 3f72-44a7-89c5-5595fe6b30ee}\shellfolder
         Opens kev:
89c5-5595fe6b30ee}\shellfolder
         Opens key:
                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 e946b44c8dd5}\shellfolder
          Opens key:
                                                                                                                                           HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 e946b44c8dd5}\shellfolder
          Opens key:
                                                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{031e4825-
  7b94-4dc3-b131-e946b44c8dd5}\shellfolder
         Opens kev:
b131-e946b44c8dd5}\shellfolder
                                                                                                                                           HKCU\software\classes\wow6432node\clsid\{04731b67-d933-450a-90e6-
        Opens kev:
 4acd2e9408fe}\shellfolder
          Opens key:
                                                                                                                                           HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 4acd2e9408fe}\shellfolder
         Opens key:
                                                                                                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{04731b67-microsoft \setminus windows \setminus current version \setminus clsid \setminus explorer \setminus clsid 
  d933-450a-90e6-4acd2e9408fe}\shellfolder
         Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (2013) \ declined \ (2013) \ declined \ decli
 90e6-4acd2e9408fe}\shellfolder
                                                                                                                                           HKCU\software\classes\wow6432node\clsid\{11016101-e366-4d22-bc06-
          Opens kev:
 4ada335c892b}\shellfolder
                                                                                                                                            HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
          Opens kev:
 4ada335c892b}\shellfolder
                                                                                                                                          HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus clsid \setminus explorer \setminus clsid 
         Opens key:
  e366-4d22-bc06-4ada335c892b}\shellfolder
         Opens kev:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{11016101-e366-4d22-
bc06-4ada335c892b}\shellfolder
                                                                                                                                           HKCU\software\classes\wow6432node\clsid\{4336a54d-038b-4685-ab02-
         Opens kev:
  99bb52d3fb8b}\shellfolder
          Opens key:
                                                                                                                                           HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
 99bb52d3fb8b}\shellfolder
                                                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\clsid\{4336a54d-
         Opens key:
  038b-4685-ab02-99bb52d3fb8b}\shellfolder
         Opens kev:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{4336a54d-038b-4685-
 ab02-99bb52d3fb8b}\shellfolder
         Opens kev:
                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
```

0800361b1103}\shellfolder

HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-Opens key: 0800361b1103}\shellfolder Opens key: ad25-11d0-98a8-0800361b1103}\shellfolder Opens kev:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{450d8fba-ad25-11d0-d848fba-ad25-11d0-d848fba-ad25-11d0-d848fba-ad25-11d0-d848fba-ad25-d848f$ 98a8-0800361b1103}\shellfolder Opens kev: HKCU\software\classes\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder Opens key: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder Opens key: 6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder HKCU\software\classes\wow6432node\clsid\{89d83576-6bd1-4c86-9454-Opens kev: beb04e94c819}\shellfolder HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-Opens key: beb04e94c819}\shellfolder HKCU\software\microsoft\windows\currentversion\explorer\clsid\{89d83576-Opens key: 6bd1-4c86-9454-beb04e94c819}\shellfolder Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{89d83576-6bd1-4c86-9454-beb04e94c819}\shellfolder  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{9343812e-1c37-4a49-a12e-$ Opens key: 4b2d810d956b}\shellfolder HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-Opens key: 4b2d810d956b}\shellfolder HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9343812e-Opens key: 1c37-4a49-a12e-4b2d810d956b}\shellfolder Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{9343812e-1c37-4a49-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7$ a12e-4b2d810d956b}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78ad1f5659cba93}\shellfolder HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-Opens kev: d1f5659cba93}\shellfolder  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{b4fb3f98-b4fb$ Opens key: c1ea-428d-a78a-d1f5659cba93}\shellfolder Opens key: a78a-d1f5659cba93}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086b309680c6b7e}\shellfolder HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-Opens key: b309680c6b7e}\shellfolder Opens key: 21cb-41b2-a086-b309680c6b7e}\shellfolder Opens key: a086-b309680c6b7e}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{daf95313-e44d-46af-be1bcbacea2c3065}\shellfolder HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-Opens kev: cbacea2c3065}\shellfolder Opens key:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{daf95313-daf9531-daf9501-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf953$ e44d-46af-be1b-cbacea2c3065}\shellfolder Opens key: be1b-cbacea2c3065}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-Opens kev: 4e922c26259e}\shellfolder Opens key: 9397-435c-8f95-4e922c26259e}\shellfolder Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{e345f35f-9397-435c-945f-9497-435c-9497-445f-947-445f-947-45f-947-445f-947-456f-947-456f-947-456f-947-4$ 8f95-4e922c26259e}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-Opens key: 96b02cfe0d52}\shellfolder Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \ed 228fdf-lem \clsid \clsi$ 9ea8-4870-83b1-96b02cfe0d52}\shellfolder Opens key: 83b1-96b02cfe0d52}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-

Opens kev:

7367fc96ef3c}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-

be21-4350-88b0-7367fc96ef3c}\shellfolder

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{f02c1a0d-be21-4350-be21-450-be21-450-be21-450-be21-450-be21-450-be21-450-be21-450-be21-450-be21-450-be21-450-b$ 

88b0-7367fc96ef3c}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\app paths\cmd.exe
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app

paths\cmd.exe

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe

Opens key:

Opens key:

11e3-a68e-806e6f6e6963}\

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ shell \ registered applications \ urlassociations \ directory \ open with progids$ 

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \microsoft \windows \shell \associations \urlassociations \directory \end{tabular}$ 

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver
Opens key: HKCR\directory\

Opens key: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler
Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder

Opens key: HKCU\software\classes\folder\shellex\iconhandler

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

Opens key: HKCU\software\classes\allfilesystemobjects\shellex\iconhandler

Opens key: HKCR\allfilesystemobjects\shellex\iconhandler
Opens key: HKCU\software\classes\directory\docobject

Opens key: HKCR\directory\docobject

Opens key: HKCU\software\classes\folder\docobject

Opens key: HKCR\folder\docobject

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCU} \\ \mathsf{software} \\ \mathsf{classes} \\ \mathsf{allfilesystemobjects} \\ \mathsf{docobject} \\$ 

Opens key: HKCR\allfilesystemobjects\docobject

Opens key: HKCU\software\classes\directory\browseinplace

Opens key: HKCR\directory\browseinplace

Opens key: HKCU\software\classes\folder\browseinplace

Opens key: HKCR\folder\browseinplace

Opens key: HKCU\software\classes\allfilesystemobjects\browseinplace

Opens key: HKCR\allfilesystemobjects\browseinplace
Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

Opens key: HKCU\software\classes\allfilesystemobjects\clsid

Opens key: HKCR\allfilesystemobjects\clsid Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\.exe\openwithprogids

Opens key: HKCR\.exe\openwithprogids

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\openwithprogids
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\

Opens key:

 $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \end{tabular} $$ exe \software \mbox{$ 

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

Opens key: HKCU\software\classes\exefile\curver

Opens key: HKCR\exefile\curver

Opens key: HKCR\exefile\

Opens key: HKCU\software\classes\exefile\shellex\iconhandler

Opens key: HKCR\exefile\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\.exe

Opens key: HKCR\systemfileassociations\.exe

Opens key: HKCU\software\classes\systemfileassociations\.exe\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.exe\shellex\iconhandler

Opens key: HKCU\software\classes\exefile\docobject
Opens key: HKCR\exefile\docobject

```
Opens key:
                                     HKCU\software\classes\systemfileassociations\.exe\docobject
  Opens key:
                                     HKCR\systemfileassociations\.exe\docobject
  Opens key:
                                     HKCU\software\classes\exefile\browseinplace
  Opens key:
                                     HKCR\exefile\browseinplace
  Opens key:
                                     HKCU\software\classes\systemfileassociations\.exe\browseinplace
  Opens key:
                                     HKCR\systemfileassociations\.exe\browseinplace
                                     HKCU\software\classes\exefile\clsid
  Opens key:
                                     HKCR\exefile\clsid
  Opens key:
  Opens key:
                                     HKCU\software\classes\systemfileassociations\.exe\clsid
  Opens key:
                                     HKCR\systemfileassociations\.exe\clsid
  Opens kev:
db2c-424c-b029-7fe99a87c641}
db2c-424c-b029-7fe99a87c641}\propertybag
                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens key:
b8dc300d9f9d}
  Opens key:
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:
                                     HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50
b8dc300d9f9d}\treatas
  Opens key:
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
                                     Opens kev:
b8dc300d9f9d}\progid
  Opens key:
                                     HKCR\wow6432 node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
                                     HKCU \setminus software \setminus classes \setminus clsid \setminus \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}
  Opens key:
  Opens key:
                                     HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
  Opens key:
                                     HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\progid
  Opens key:
                                     HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
  Opens key:
                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:
  Opens key:
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                     HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version
  Opens key:
                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens kev:
b8dc300d9f9d}\inprochandler32
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens key:
b8dc300d9f9d}\inprochandler32
  Opens key:
                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Opens kev:
b8dc300d9f9d}\inprochandler
  Opens kev:
11e3-a68e-806e6f6e6963}\
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}
b587-4786-b4ef-bd1dc332aeae}\propertybag
                                     HKLM\software\microsoft\windows\currentversion\explorer\kindmap
  Opens key:
  Opens key:
                                     HKCU\software\classes\exefile\shell
  Opens key:
                                     HKCR\exefile\shell
  Opens key:
                                     HKCU\software\classes\exefile\shell\open
  Opens key:
                                     HKCR\exefile\shell\open
  Opens key:
                                     HKCR\exefile\shell\open\
  Opens key:
                                     HKCU\software\classes\exefile\shell\open\command
  Opens key:
                                     HKCR\exefile\shell\open\command
  Opens key:
                                     \label{loopendroptarget} \mbox{HKCU\software\classes\exefile\shell\open\droptarget} \\
  Opens key:
                                     HKCR\exefile\shell\open\droptarget
  Opens key:
HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| policies\\| associations
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\policies\associations
                                     \label{thm:local_hammon} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc policies\associations}} \label{thm:local_hammon}
  Opens key:
  Opens key:
                                     HKCU\software\classes\.ade
  Opens key:
                                     HKCR\.ade
                                     HKCU\software\classes\.adp
  Opens kev:
  Opens key:
                                     HKCR\.adp
  Opens key:
                                     HKCU\software\classes\.app
  Opens key:
                                     HKCR\.app
  Opens key:
                                     HKCU\software\classes\.asp
  Opens key:
                                     HKCR\.asp
  Opens key:
                                     HKCU\software\classes\.bas
```

Opens key: HKCR\.bas

Opens key: HKCU\software\classes\.bat

Opens key: HKCR\.bat

Opens key: HKCU\software\classes\.cer

Opens key: HKCR\.cer

Opens key: HKCU\software\classes\.chm

Opens key: HKCR\.chm

HKCU\software\classes\.cmd Opens key: Opens key: HKCR\.cmd HKCU\software\classes\.com Opens kev: Opens key: HKCR\.com Opens key: HKCU\software\classes\.cpl Opens key: HKCR\.cpl HKCU\software\classes\.crt Opens key: Opens key: HKCR\.crt Opens key: HKCU\software\classes\.csh Opens key: HKCR\.csh Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\treatas  $HKCR\wow6432 node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treat as$ Opens key: Opens kev: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid Opens key:  $HKCR\wow6432 node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid$ HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{7b8a2d94 - 0ac9 - 11d1 - 896c - 11d1 - 806c - 11d1 - 806c$ Opens kev: 00c04fb6bfc4}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\inprochandler HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens key: 00c04fb6bfc4}\inprochandler HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_zones\_default\_drive\_intranet\_kb941000 HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_zones\_default\_drive\_intranet\_kb941000 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_protocol\_lockdown Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens kev: settings\zones\0 Opens key: HKCU\software\classes\exefile\progid Opens key: HKCR\exefile\progid Opens key:  $HKLM \label{loop} IkLM \label{loop} HKLM \label{loop} Which software \label{loop} Wh$ Opens kev: HKCU\software\classes\exefile\shell\open\ddeexec Opens key: HKCR\exefile\shell\open\ddeexec Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmd.exe HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe Opens key: HKLM\software\wow6432node\microsoft\windows Opens key: HKLM\software\wow6432node\microsoft\windows\html help Opens key: HKLM\software\wow6432node\microsoft\windows\help Opens key: HKCU\software\policies\microsoft\windows\system Opens key:  $HKLM \backslash software \backslash wow 6432 node \backslash microsoft \backslash command processor$ Opens key: HKCU\software\microsoft\command processor Opens key: options\tasklist.exe Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\tasklist.exe Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder Opens key: HKLM\software\wow6432node\microsoft\wbem\cimom HKLM\system\currentcontrolset\services\lanmanworkstation\parameters Opens kev:

HKLM\software\microsoft\windows nt\currentversion\image file execution HKCU\software\classes\appid\tasklist.exe Opens key: Opens key: HKCR\appid\tasklist.exe Opens key: HKLM\system\currentcontrolset\control\lsa Opens key: 00aa004b2e24} HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens kev: Opens key: 

00aa004b2e24}\treatas

 Opens key:
 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f

00aa004b2e24}\progid

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\progid

Opens key: HKCR\clsid\\4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\\4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler

Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters

Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}

00c04fb68820}\treatas

Opens key:  $\begin{tabular}{ll} HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treat as Opens key: \\ HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-d86$ 

00c04fb68820}\progid

 $\label{lem:continuous} Opens key: $$ HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid $$ Opens key: $$ HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}$$$ 

 Opens key:
 HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}

 Opens key:
 HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075

00c04fb68820}\progid

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

 $00c04fb68820 \} \verb|\inprochandler32| \\$ 

Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler

Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler

Opens key:

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Wow 6432 node \label{lem:hklm} icrosoft \label{lem:hklm} cryptography \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hkklm} \lab$ 

provider

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

Opens key:

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload

000000000046}

 $000000000046 \} \ proxystubcl sid 32$ 

Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-

 $000000000046 \} \ proxystubcl sid 32$ 

Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions

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

Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-

00c04fb68820}

Opens key:  $\begin{tabular}{ll} HKCR\wow6432node\interface\f309ad18-d86a-11d0-a075-00c04fb68820\} \\ Opens key: \\ HKCU\software\classes\wow6432node\interface\f309ad18-d86a-11d0-a075-00c04fb68820\} \\ \end{tabular}$ 

00c04fb68820}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-

00c04fb68820}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}

Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-

Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\progid

00aa004b2e24}\treatas

 $HKCR\wow6432 node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid$ Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid Opens key:  $\label{local-condition} HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid$ Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32 Opens key:  $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-8$ 00aa004b2e24}\inprochandler HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens kev: 00aa004b2e24}\inprochandler Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32 Opens key: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32 HKLM\system\currentcontrolset\control\computername Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid  $HKCR\wow6432 node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid$ Opens key: Opens key: HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\progid HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid Opens key: Opens key HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprochandler HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprochandler Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} Opens kev: Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32 HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-Opens key 00aa003240c7}\proxystubclsid32  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{d68af00a-29cb-43fa-8504-468af00a-29cb-436af00a-29$ Opens key: ce99a996d9ea}  $HKCR \ wow 6432 node \ clsid \ \{d68af00a-29cb-43fa-8504-ce99a996d9ea\}$ Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea}\treatas  $HKCR \setminus wow6432 node \\ clsid \\ \{d68af00a-29cb-43fa-8504-ce99a996d9ea\} \\ \setminus treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea}\progid  $HKCR\wow6432 node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\$ Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{d68af00a-29cb-43fa-8504-ce99a996d9ea\}$ HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens kev:

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\progid

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid Opens kev:

Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504er32

ce99a996d9ea}\inprocserv

Opens kev: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler32

Opens kev:

ce99a996d9ea}\inprochandler

Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler

Opens key: HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-

00000000001}

000000000001}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-

00000000001}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}

 Opens key:
 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

00104b703efd}\treatas

Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas Opens key: HKCU\software\clsid\frac{1}{2} Opens key: HKCU\sof

00104b703efd}\progid

Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

 Opens key:
 HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

 Opens key:
 HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

00104b703efd}\progid

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler

Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler

Opens key: HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}

Opens key: HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}

 Opens key:
 HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}

 Opens key:
 HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-0014b703efd}

00104b703efd}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}

 $\label{lem:continuous} Opens key: $$ HKCR\wow6432node\clsid\eb87e1bd-3233-11d2-aec9-00c04fb68820} $$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\eb87e1bd-3233-11d2-aec9-$ 

00c04fb68820}\treatas

 $\label{lem:continuous} Opens~key: $$ HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas $$ Opens~key: $$ HKCU\software\classes\wow6432node\clsid\end{array}$$ Opens~key: $$ O$ 

00c04fb68820}\progid

Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\progid Opens key: HKCU\software\classes\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\
Opens key: HKCP\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\
Opens key: HKCP\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\

 Opens key:
 HKCR\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}

 Opens key:
 HKCU\software\classes\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}

00c04fb68820}\progid

Opens key: HKCR\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprochandler

Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprochandler

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

options[disableusermodecallbackfilter]

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]$ 

Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Oueries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Queries value:

Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

HKCU\control panel\desktop[preferreduilanguages] Oueries value:

Oueries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side [prefer external manifest]$ 

HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[usefilter]

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

options\dllnxoptions[msvbvm60.dll]

HKI M\software\microsoft\windows Queries value: nt\currentversion\gre\_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[f0d96afe8a3c58bf99f8b24ff10b1a07] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

 ${\tt HKLM \backslash software \backslash microsoft \backslash ole[pageallocator use system heap]}$ Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932] Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949] HKLM\system\currentcontrolset\control\nls\codepage[950] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]

Queries value: HKLM\software\microsoft\com3[com+enabled] Oueries value: HKLM\software\microsoft\ole[maxsxshashcount] HKLM\system\currentcontrolset\services\disk\enum[0] Queries value:

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Oueries value:

HKLM\system\setup[oobeinprogress] Oueries value: Oueries value: HKLM\system\setup[systemsetupinprogress]

HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries value:

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value:

settings[security\_hklm\_only]

HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings[fromcachetimeout]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[secureprotocols]

HKCU\software\policies\microsoft\windows\currentversion\internet Oueries value:

settings[secureprotocols]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value:

settings[secureprotocols]

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}$ Oueries value: settings[certificaterevocation]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[disablekeepalive] HKCU\software\microsoft\windows\currentversion\internet

Queries value:

settings[disablepassport]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]

Queries value:

 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings[enablehttp1\_1]

Queries value:

settings[enablehttp1\_1] Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings[enablehttp1\_1]

Queries value:  $\label{lem:hklmsoftware bolicies microsoft windows \current version \cite{thmsoftware} in the lemma of the$ 

settings[proxyhttp1.1]

HKCU\software\policies\microsoft\windows\currentversion\internet

HKCU\software\policies\microsoft\windows\currentversion\internet

Queries value:

settings[proxyhttp1.1] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings[proxyhttp1.1]

Queries value:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ 

settings[enablenegotiate]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel]

HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol[feature\_clientauthcertfilter]

HKLM\software\wow6432node\microsoft\internet Queries value:

explorer\main\featurecontrol[feature\_clientauthcertfilter]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[clientauthbuiltinui]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings[syncmode5]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Queries value:

settings\5.0\cache[signature]

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version \hammon_h$ Queries value:

settings\5.0\cache\content[peruseritem]

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\content[peruseritem]

Queries value:

33be-4251-ba85-6007caedcf9d}[category]

33be-4251-ba85-6007caedcf9d}[name]

33be-4251-ba85-6007caedcf9d}[parentfolder]

33be-4251-ba85-6007caedcf9d}[description]

33be-4251-ba85-6007caedcf9d}[relativepath]

33be-4251-ba85-6007caedcf9d}[parsingname]

33be-4251-ba85-6007caedcf9d}[infotip]

33be-4251-ba85-6007caedcf9d}[localizedname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]

Oueries value:

33be-4251-ba85-6007caedcf9d}[security]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]

Oueries value:

33be-4251-ba85-6007caedcf9d}[streamresourcetype]

33be-4251-ba85-6007caedcf9d}[localredirectonly]

Oueries value:

33be-4251-ba85-6007caedcf9d}[roamable]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]

33be-4251-ba85-6007caedcf9d}[publishexpandedpath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]

33be-4251-ba85-6007caedcf9d}[foldertypeid]

Queries value:

33be-4251-ba85-6007caedcf9d}[initfolderhandler]

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

folders[cache]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b$ 6fba-4fcf-9d55-7b8e7f157091}[category]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]

Oueries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[description]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [relative path]$ 

Oueries value

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [localized name]$ 

Oueries value

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$ 

Oueries value.

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource type]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [local redirectonly]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [roamable]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [precreate]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{f1b32785-6fba-4fcf-9d55-7b8e7f157091} [publish expanded path]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\fifth 32785-66ba-4fcf-9d55-7b8e7f157091\fifth 157091\fifth 157091\$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [folder typeid]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \mbox{f1b32785-6fba-4fcf-9d55-7b8e7f157091} [initfolder handler]$ 

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

folders[local appdata]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions \currentversion\explorer\folderdescriptions \currentversion\explorer\folderdescription \currentversion\explorer\folderdescription \currentversion\explorer\folderdescription\explorer\folderdescription \currentversion\explorer\folderdescription\explorer\folderd$ 

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folde$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Queries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localized name]}$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [security]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource type]$ 

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [local redirector \ local \ local redirector \ local redirector \ local \ l$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [roamable]$ 

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [precreate]$ 

Oueries value

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [attributes]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [folder type id]$ 

Queries value

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001[profileimagepath]

 $\label{thm:consoftware} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$ 

settings\5.0\cache\content[cacheprefix]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cachelimit]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[peruseritem]

Queries value:

 $\label{local-observation} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \cdot\$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folder descriptions \cdot \c$ 

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [relative path]$ 

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[parsingname]}$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [localized name]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]$ 

Queries value:

Oueries value:

 $HKLM\software\swow6432 node\swireosoft\swindows\currentversion\explorer\folderdescriptions\folderdescripti$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\explorer\folderdescriptions\currentversion\explorer\$ 

Queries value:

 $\label{thm:hammon} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cal{thm:hammon} \cline{2b0f765d-1000} \cline{2b0f765d-10000} \cline{2b0f765d-10000} \cline{2b0f765d-10000} \cline{2b0f765d-10000} \cline{2b0f765$ 

c0e9-4171-908e-08a611b84ff6}[localredirectonly]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [roamable]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [publish \ expanded \ path \ ]$ 

Oueries value:

 $\label{local-HKLM} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe9-4171-90$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [folder type id]$ 

Queries value:

 $\label{limit} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[initfolderhandler]}$ 

Queries value:

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

folders[cookies]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [category]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [name]$ 

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [description]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[parsingname]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 6569-4cf6-a03a-e3ef65729f3d \cite{linfotip} \end{substitute}$ 

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [icon]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}\\[security]$ 

Queries value:

 $\label{lem:hamman} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresource]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f$ 

Queries value:

 $\label{local_HKLM} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[roamable]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [precreate]$ 

Oueries value:

 $HKLM \\ software \\ \\ wow 6432 \\ node \\ microsoft \\ windows \\ current \\ version \\ explorer \\ folder \\ descriptions \\ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[stream]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \fol$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [attributes]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [folder type id]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ between the sum of the$ 

65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[cacheprefix]

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Queries value:

settings\5.0\cache\cookies[cachelimit]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\history[peruseritem]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d12b, d12b, d24b, d$ b784-432e-a781-5a1130a75963}[category]

Queries value:

b784-432e-a781-5a1130a75963}[name]

Queries value:

b784-432e-a781-5a1130a75963}[parentfolder]

b784-432e-a781-5a1130a75963}[description]

b784-432e-a781-5a1130a75963}[relativepath]

b784-432e-a781-5a1130a75963}[parsingname]

b784-432e-a781-5a1130a75963}[infotip]

b784-432e-a781-5a1130a75963}[localizedname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[icon]

Queries value:

b784-432e-a781-5a1130a75963}[security]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[streamresource]

Oueries value:

b784-432e-a781-5a1130a75963}[streamresourcetype]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[localredirectonly] Oueries value:

b784-432e-a781-5a1130a75963}[roamable] Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[precreate]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[stream]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[publishexpandedpath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[attributes]

b784-432e-a781-5a1130a75963}[foldertypeid]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d9dc8a1b-d$ b784-432e-a781-5a1130a75963}[initfolderhandler]

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

folders[history]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history[cacheprefix]

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Oueries value:

settings\5.0\cache\history[cachelimit]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\domstore[cacherepair]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\extensible cache\domstore[cachepath]

HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings\5.0\cache\extensible cache\domstore[cacheprefix]

```
Oueries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
   Oueries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
   Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
   Queries value:
                                                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma of the 
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
   Oueries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
   Queries value:
                                                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                                                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \normalises \policies \microsoft \windows \normalises \policies \
   Oueries value:
settings[enableautoproxyresultcache]
   Queries value:
                                                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
settings[displayscriptdownloadfailureui]
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[mbcsservername]
                                                           \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu
   Oueries value:
settings[mbcsapiforcrack]
   Queries value:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disableworkerthreadhibernation]
   Oueries value:
                                                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
   Oueries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[socketsendbufferlength]
                                                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
   Queries value:
settings[socketreceivebufferlength]
   Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxhttpredirects]
   Queries value:
                                                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[maxconnectionsperserver]
   Queries value:
                                                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[maxconnectionsperserver]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[maxconnectionsper1_0server]
   Queries value:
                                                           HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet
settings[maxconnectionsper1_0server]
   Queries value:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[serverinfotimeout]
   Queries value:
                                                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[connecttimeout]
   Queries value:
                                                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
```

```
settings[connecttimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[receivetimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                         HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirvtimesecs]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[f0d96afe8a3c58bf99f8b24ff10b1a07.exe]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                         settings[bypasssslnocachecheck]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnalwaysonpost]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertrecving] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnonpostredirect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[tcpautotuning] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000001[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002[packedcatalogitem] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000003[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[packedcatalogitem] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num] Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5[num\_catalog\_entries]$ Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 00000000001[library path]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[enabled] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo] Queries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 000000000002[library path])$ Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000002 \ [displaystring]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 000000000000000[enabled]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 00000000000002[provider info]$ 

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog \ entries \ 00000000000002 \ [storesservice class in fo]$ 

Oueries value:

Queries value:

Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath] Oueries value:
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring] Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000004 \ [providerid] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
  Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog \catalog\_entries \namespace\_entries \na$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings\wpad[wpadoverride]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[enableautodial]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[nonetautodial]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[globaluseroffline]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[badproxyexpirestime]

Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disablebranchcache] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_http\_username\_password\_disable[f0d96afe8a3c58bf99f8b24ff10b1a07.exe] Oueries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_http\_username\_password\_disable[\*] Oueries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing] Oueries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ fod 96afe 8a 3c 58bf 99f8b 24ff 10b1 a 07\_rasapi 32[enable file tracing]$ Oueries value:  $HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus tracing \setminus fod96 \\ afe8a3c58bf99f8b24ff10b1a07\_rasapi32[filetracingmask]$ Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus fod 96afe 8a 3c 58bf 99f8b 24ff 10b 1a07\_rasapi 32[enable consolet racing]$ Oueries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ fod 96afe 8a3c 58bf 99f8b 24ff 10b1a07\_rasapi 32[consoletracing mask]$ Oueries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ fod 96afe 8a 3c 58bf 99f8b 24ff 10b1a07\_rasapi 32[maxfilesize]$ Queries value: HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[filedirectory] Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ fod 96afe 8a 3c 58bf 99f8b 24ff 10b1 a 07\_rasmancs \ [enable file tracing]$ Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus f0d96afe8a3c58bf99f8b24ff10b1a07\_rasmancs[filetracingmask]$  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus fod 96 af e8a3c58bf 99f8b24ff 10b1a07\_rasmancs [enable consolet racing]$ Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus fod 96afe 8a 3c 58bf 99f8b 24ff 10b 1a 07\_ras mancs [consolet racing mask]$ Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus fod96afe8a3c58bf99f8b24ff10b1a07\_rasmancs [maxfilesize]$ HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasmancs[filedirectory] Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] HKLM\software\microsoft\windows nt\currentversion\profilelist[programdata] Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[7393e979] Queries value: HKLM\software\microsoft\samclient\windows\disabledsessions[machinethrottling] Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[proxysettingsperuser] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[savedlegacysettings] Queries value:  $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ settings\connections[defaultconnectionsettings] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]  $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dynamicser verquery order]$ 

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[useedns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]  $\label{lem:hklmsystem} \verb|HKLM| system| current control set | services| dnscache| parameters [use hosts file]| \\$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]$ Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatetop]eveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [enable multicast]$ Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]

Oueries value:

```
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mime_handling[f0d96afe8a3c58bf99f8b24ff10b1a07.exe]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
 Queries value:
                          HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\\ main\feature control\feature unc\_saved file check [f0d96afe8a3c58bf99f8b24ff10b1a07.exe]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
                          HKLM\software\policies\microsoft\internet
 Queries value:
explorer\security[disablesecuritysettingscheck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\2[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[f0d96afe8a3c58bf99f8b24ff10b1a07.exe]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                          HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[f0d96afe8a3c58bf99f8b24ff10b1a07.exe]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
 Queries value:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[enablepunycode]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablepunycode]
 Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                          HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value:
                          HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
                          HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
 Queries value:
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[1a10]
 Queries value:
                          HKLM\system\currentcontrolset\services\winsock\parameters[transports]
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                          HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [mapping]
 Queries value:
                          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                          HKLM\system\currentcontrolset\services\winsock\setup
 Oueries value:
migration\providers\tcpip6[winsock 2.0 provider id]
```

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]

Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value:

Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[searchlist]

Queries value:

e1e01c1f69b5}[enabledhcp]

Queries value:

e1e01c1f69b5}[registrationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registeradaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[domain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpdomain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpv6domain]

Queries value:

e1e01c1f69b5}[nameserver]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[nameserver]

Queries value:

e1e01c1f69b5}[dhcpnameserver]

Oueries value:

806e6f6e6963}[enabledhcp]

Queries value:

806e6f6e6963}[registrationenabled]

Oueries value:

806e6f6e6963}[registeradaptername]

Oueries value:

806e6f6e6963}[domain]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]

Queries value:

806e6f6e6963}[nameserver]

Queries value:

806e6f6e6963}[dhcpnameserver]

HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value:

Queries value:

e1e01c1f69b5}[queryadaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[disableadapterdomainname]

Queries value:

e1e01c1f69b5}[registrationmaxaddresscount]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[maxnumberofaddressestoregister]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[enablemulticast]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]

Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disableadapterdomainname]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enableadapterdomainnameregistration]
 Oueries value:
```

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddressestoregister]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export] Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks] Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]

HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]

HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lklm} HKLM \label{lklm} White \label{lklm} White \label{lklm} HKLM \label{lklm} White \label{lklm} HKLM \label{lklm} White \label{lklm} HKLM \label{lklm} White \label{lklm} White \label{lklm} HKLM \label{lklm} White \label{lklm} HKLM \label{lklm} White \label{lklm} W$ 7b94-4dc3-b131-e946b44c8dd5}[suppressionpolicy]

Queries value:

d933-450a-90e6-4acd2e9408fe}[suppressionpolicy]

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem$ e366-4d22-bc06-4ada335c892b}[suppressionpolicy]

Queries value:

a00a-44d7-9371-beb064c98683}[suppressionpolicy]

Oueries value:

038b-4685-ab02-99bb52d3fb8b}[suppressionpolicy]

Oueries value:

ad25-11d0-98a8-0800361b1103}[suppressionpolicy]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}[suppressionpolicy]

Oueries value:

3f72-44a7-89c5-5595fe6b30ee}[suppressionpolicy]

Queries value:

5081-101b-9f08-00aa002f954e}[suppressionpolicy]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ namespace \ \{89d83576-1964, 1$ 6bd1-4c86-9454-beb04e94c819}[suppressionpolicy]

Queries value:

 $HKLM \label{lem:hklm} Which is the software \label{lem:hkklm} Which is the software \label{l$ 1c37-4a49-a12e-4b2d810d956b}[suppressionpolicy]

Oueries value:

c1ea-428d-a78a-d1f5659cba93}[suppressionpolicy]

Oueries value:

21cb-41b2-a086-b309680c6b7e}[suppressionpolicy]

Oueries value:

e44d-46af-be1b-cbacea2c3065}[suppressionpolicy]

Oueries value:

9397-435c-8f95-4e922c26259e}[suppressionpolicy]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ namespace \ \{ed 228 fdf-desktop \ namespace \ ed 228 fdf-desktop \ n$ 

```
9ea8-4870-83b1-96b02cfe0d52}[suppressionpolicy]
  Oueries value:
be21-4350-88b0-7367fc96ef3c}[suppressionpolicy]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[attributes]
  Oueries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
  Oueries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
  Queries value:
                                   08002b30309d}\shellfolder[usedrophandler]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
                                   Queries value:
08002b30309d}\shellfolder[queryforoverlay]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[queryforinfotip]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[hideinwebview]
                                   Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Oueries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}1
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Queries value:
08002b30309d}\shellfolder[attributes]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Queries value:
08002b30309d}\shellfolder[callforattributes]
                                   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[wantsfordisplay]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Queries value:
08002b30309d}\shellfolder[usedrophandler]
  Queries value:
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[wantsforparsing]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Queries value:
08002b30309d}\shellfolder[queryforoverlay]
  Oueries value:
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[mapnetdriveverbs]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
  Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[nofilefolderjunction]
  Oueries value:
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[pintonamespacetree]
  Oueries value:
                                   HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{208d2c60-3aea-1069-a2d7-
08002b30309d}1
  Queries value:
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
```

```
08002b30309d}\shellfolder[attributes]
                                                        Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\shellfolder[restrictedattributes]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsfordisplay]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
    Oueries value:
                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[usedrophandler]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsforparsing]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforoverlay]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideinwebview]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hasnavigationenum]
                                                         HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid 
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea
08002b30309d}1
    Queries value:
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\inprocserver32[loadwithoutcom]
                                                        HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0xffff]
    Queries value:
                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\[]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
    Oueries value:
08002b30309d}\inprocserver32[threadingmodel1
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[attributes]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
   Oueries value:
00aa002f954e}\shellfolder[callforattributes]
    Oueries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[restrictedattributes]
    Oueries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[wantsfordisplay]
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[hidefolderverbs]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
    Queries value:
00aa002f954e}\shellfolder[usedrophandler]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
    Oueries value:
00aa002f954e}\shellfolder[wantsforparsing]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
    Queries value:
OOaaOO2f954e}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[queryforoverlay]
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[mapnetdriveverbs]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
    Oueries value:
00aa002f954e}\shellfolder[queryforinfotip]
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[hideinwebview]
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[hideondesktopperuser]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
   Oueries value:
00aa002f954e}\shellfolder[wantsaliasednotifications]
    Queries value:
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[wantsuniversaldelegate]
    Queries value:
                                                         HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
```

```
00aa002f954e}\shellfolder[nofilefolderjunction]
                                                       HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
    Oueries value:
00aa002f954e}\shellfolder[pintonamespacetree]
                                                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
    Queries value:
00aa002f954e}\shellfolder[hasnavigationenum]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{645ff040-5081-101b-9f08-
00aa002f954e}1
    Oueries value:
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[attributes]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[callforattributes]
    Queries value:
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[restrictedattributes]
    Queries value:
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[wantsfordisplay]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[hidefolderverbs]
    Queries value:
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[usedrophandler]
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Queries value:
beb064c98683}\shellfolder[wantsforparsing]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[wantsparsedisplayname]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Queries value:
beb064c98683}\shellfolder[queryforoverlay]
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Queries value:
beb064c98683}\shellfolder[mapnetdriveverbs]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[queryforinfotip]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[hideinwebview]
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Queries value:
beb064c98683}\shellfolder[hideondesktopperuser]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[wantsaliasednotifications]
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[wantsuniversaldelegate]
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Queries value:
beb064c98683}\shellfolder[nofilefolderjunction]
    Queries value:
                                                       HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[pintonamespacetree]
                                                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
    Oueries value:
beb064c98683}\shellfolder[hasnavigationenum]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-9371-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{26ee0668-a00a-44d7-microsoft \setminus current version \setminus curr
beb064c98683}]
    Queries value:
                                                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[attributes]
    Queries value:
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[callforattributes]
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[restrictedattributes]
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[wantsfordisplay]
    Queries value:
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[hidefolderverbs]
                                                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[usedrophandler]
                                                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[wantsforparsing]
    Oueries value:
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[wantsparsedisplayname]
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[queryforoverlay]
                                                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[mapnetdriveverbs]
                                                       HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
    Queries value:
5595fe6b30ee}\shellfolder[queryforinfotip]
                                                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[hideinwebview]
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[hideondesktopperuser]
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[wantsaliasednotifications]
    Oueries value:
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[nofilefolderjunction]
    Oueries value:
                                                       HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[pintonamespacetree]
                                                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
```

5595fe6b30ee}\shellfolder[hasnavigationenum]

```
Oueries value:
5595fe6b30ee}1
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[attributes]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Oueries value:
e946b44c8dd5}\shellfolder[restrictedattributes]
 Oueries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[wantsfordisplay]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[hidefolderverbs]
 Oueries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[usedrophandler]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[wantsforparsing]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[wantsparsedisplayname]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Oueries value:
e946b44c8dd5}\shellfolder[queryforoverlay]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[mapnetdriveverbs]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[queryforinfotip]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[hideinwebview]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[hideondesktopperuser]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[wantsaliasednotifications]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[wantsuniversaldelegate]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[nofilefolderjunction]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[pintonamespacetree]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[hasnavigationenum]
 Queries value:
e946b44c8dd5}1
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[attributes]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[callforattributes]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[wantsfordisplay]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[hidefolderverbs]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[usedrophandler]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[wantsforparsing]
 Oueries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[wantsparsedisplayname]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[queryforoverlay]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Queries value:
4acd2e9408fe}\shellfolder[mapnetdriveverbs]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Queries value:
4acd2e9408fe}\shellfolder[quervforinfotip]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[hideinwebview]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Queries value:
4acd2e9408fe}\shellfolder[hideondesktopperuser]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[wantsaliasednotifications]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[wantsuniversaldelegate]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[nofilefolderjunction]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[pintonamespacetree]
 Queries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{04731b67-d933-450a-90e6-
4acd2e9408fe}]
                        HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
 Oueries value:
4ada335c892b}\shellfolder[attributes]
```

```
Queries value:
                                       HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[callforattributes]
  Oueries value:
                                       HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[restrictedattributes]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Oueries value:
4ada335c892b}\shellfolder[wantsfordisplay]
  Queries value:
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[hidefolderverbs]
  Queries value:
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[usedrophandler]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Oueries value:
4ada335c892b}\shellfolder[wantsforparsing]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Queries value:
4ada335c892b}\shellfolder[wantsparsedisplayname]
                                       HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Queries value:
4ada335c892b}\shellfolder[queryforoverlay]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Oueries value:
4ada335c892b}\shellfolder[mapnetdriveverbs]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Queries value:
4ada335c892b}\shellfolder[queryforinfotip]
                                       HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Queries value:
4ada335c892b}\shellfolder[hideinwebview]
                                      HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
  Oueries value:
4ada335c892b}\shellfolder[hideondesktopperuser]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Queries value:
4ada335c892b}\shellfolder[wantsaliasednotifications]
                                       HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Queries value:
4ada335c892b}\shellfolder[wantsuniversaldelegate]
  Oueries value:
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[nofilefolderjunction]
                                      HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
  Oueries value:
4ada335c892b}\shellfolder[pintonamespacetree]
                                       HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{11016101-e366-4d22-bc06-
4ada335c892b}1
  Queries value:
                                       HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[attributes]
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Queries value:
99bb52d3fb8b}\shellfolder[callforattributes]
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Queries value:
99bb52d3fb8b}\shellfolder[restrictedattributes]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[wantsfordisplay]
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Queries value:
99bb52d3fb8b}\shellfolder[hidefolderverbs]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[usedrophandler]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[wantsforparsing]
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Oueries value:
99bb52d3fb8b}\shellfolder[wantsparsedisplayname]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[queryforoverlay]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[mapnetdriveverbs]
                                       HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Oueries value:
99bb52d3fb8b}\shellfolder[queryforinfotip]
                                       HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Queries value:
99bb52d3fb8b}\shellfolder[hideinwebview]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[hideondesktopperuser]
                                       HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Oueries value:
99bb52d3fb8b}\shellfolder[wantsaliasednotifications]
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Oueries value:
99bb52d3fb8b}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                      HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[nofilefolderjunction]
                                       HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  Oueries value:
99bb52d3fb8b}\shellfolder[pintonamespacetree]
  Oueries value:
                                       HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[hasnavigationenum]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{4336a54d-038b-4685-ab02-
99bb52d3fb8b}1
  Queries value:
                                       HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[attributes]
                                      HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
  Oueries value:
0800361b1103}\shellfolder[callforattributes]
  Queries value:
                                      HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[restrictedattributes]
  Queries value:
                                       HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
```

```
0800361b1103}\shellfolder[wantsfordisplay]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Oueries value:
0800361b1103}\shellfolder[hidefolderverbs]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Queries value:
0800361b1103}\shellfolder[usedrophandler]
   Queries value:
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[wantsforparsing]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Oueries value:
0800361b1103}\shellfolder[wantsparsedisplayname]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[queryforoverlay]
   Queries value:
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[mapnetdriveverbs]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Oueries value:
0800361b1103}\shellfolder[queryforinfotip]
   Queries value:
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[hideinwebview]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Queries value:
0800361b1103}\shellfolder[hideondesktopperuser]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Oueries value:
0800361b1103}\shellfolder[wantsaliasednotifications]
   Queries value:
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[wantsuniversaldelegate]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Queries value:
0800361b1103}\shellfolder[nofilefolderjunction]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Queries value:
0800361b1103}\shellfolder[pintonamespacetree]
                                                 HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
   Queries value:
0800361b1103}\shellfolder[hasnavigationenum]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{450d8fba-ad25-11d0-98a8-
0800361b1103}1
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Queries value:
1d8870fdcba0}\shellfolder[attributes]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[callforattributes]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[restrictedattributes]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Queries value:
1d8870fdcba0}\shellfolder[wantsfordisplay]
   Oueries value:
                                                 HKCR \land wow 6432 node \land clsid \land \{5399e694-6ce5-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fc
1d8870fdcba0}\shellfolder[hidefolderverbs]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[usedrophandler]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[wantsforparsing]
   Queries value:
                                                 HKCR \land wow 6432 node \land clsid \land \{5399e694-6ce5-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fce-4d6c-8fc
1d8870fdcba0}\shellfolder[wantsparsedisplayname]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[queryforoverlay]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[mapnetdriveverbs]
   Queries value:
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[queryforinfotip]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[hideinwebview]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[hideondesktopperuser]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Oueries value:
1d8870fdcba0}\shellfolder[wantsaliasednotifications]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Queries value:
1d8870fdcba0}\shellfolder[wantsuniversaldelegate]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Queries value:
1d8870fdcba0}\shellfolder[nofilefolderjunction]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[pintonamespacetree]
                                                 HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
   Queries value:
1d8870fdcba0}\shellfolder[hasnavigationenum]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}]
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[attributes]
   Queries value:
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[callforattributes]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[restrictedattributes]
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[wantsfordisplay]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[hidefolderverbs]
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[usedrophandler]
```

```
Queries value:
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsforparsing]
   Oueries value:
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsparsedisplayname]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[queryforoverlay]
   Queries value:
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[mapnetdriveverbs]
   Queries value:
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[queryforinfotip]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[hideinwebview]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Queries value:
beb04e94c819}\shellfolder[hideondesktopperuser]
   Queries value:
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsaliasednotifications]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[wantsuniversaldelegate]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Queries value:
beb04e94c819}\shellfolder[nofilefolderjunction]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Queries value:
beb04e94c819}\shellfolder[pintonamespacetree]
                                                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Oueries value:
beb04e94c819}\shellfolder[hasnavigationenum]
   Queries value:
beb04e94c819}]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[attributes]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[callforattributes]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[restrictedattributes]
   Queries value:
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[wantsfordisplay]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[hidefolderverbs]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[usedrophandler]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[wantsforparsing]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[wantsparsedisplayname]
   Queries value:
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[queryforoverlay]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[mapnetdriveverbs]
   Queries value:
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[queryforinfotip]
   Queries value:
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[hideinwebview]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Oueries value:
4b2d810d956b}\shellfolder[hideondesktopperuser]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[wantsaliasednotifications]
   Queries value:
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[wantsuniversaldelegate]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Oueries value:
4b2d810d956b}\shellfolder[nofilefolderjunction]
                                                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[pintonamespacetree]
                                                HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
   Queries value:
4b2d810d956b}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{9343812e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37
4b2d810d956b}1
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Queries value:
d1f5659cba93}\shellfolder[attributes]
   Queries value:
                                                d1f5659cba93}\shellfolder[callforattributes]
                                                Queries value:
d1f5659cba93}\shellfolder[restrictedattributes]
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Oueries value:
d1f5659cba93}\shellfolder[wantsfordisplay]
   Queries value:
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[hidefolderverbs]
   Queries value:
                                                d1f5659cba93}\shellfolder[usedrophandler]
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Oueries value:
d1f5659cba93}\shellfolder[wantsforparsing]
                                                Queries value:
d1f5659cba93}\shellfolder[wantsparsedisplayname]
   Queries value:
```

```
d1f5659cba93}\shellfolder[queryforoverlay]
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Oueries value:
d1f5659cba93}\shellfolder[mapnetdriveverbs]
   Queries value:
                                                 HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[queryforinfotip]
   Queries value:
                                                d1f5659cba93}\shellfolder[hideinwebview]
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Oueries value:
d1f5659cba93}\shellfolder[hideondesktopperuser]
   Queries value:
                                                 HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[wantsaliasednotifications]
                                                Queries value:
d1f5659cba93}\shellfolder[wantsuniversaldelegate]
   Queries value:
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[nofilefolderjunction]
   Queries value:
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[pintonamespacetree]
                                                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Queries value:
d1f5659cba93}\shellfolder[hasnavigationenum]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[attributes]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Queries value:
b309680c6b7e}\shellfolder[callforattributes]
                                                 HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Queries value:
b309680c6b7e}\shellfolder[restrictedattributes]
   Oueries value:
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[wantsfordisplay]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[hidefolderverbs]
                                                 HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Queries value:
b309680c6b7e}\shellfolder[usedrophandler]
   Oueries value:
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[wantsforparsing]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[wantsparsedisplayname]
                                                 HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Queries value:
b309680c6b7e}\shellfolder[queryforoverlay]
   Queries value:
                                                HKCR \land bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[mapnetdriveverbs]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[queryforinfotip]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[hideinwebview]
   Queries value:
                                                HKCR \land bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[hideondesktopperuser]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[wantsaliasednotifications]
   Oueries value:
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[wantsuniversaldelegate]
   Queries value:
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[nofilefolderjunction]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[pintonamespacetree]
                                                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[hasnavigationenum]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}1
                                                 HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{daf95313 - e44d - 46af - be1b - e44d - e46af - e46af - e44d - e46af -
   Queries value:
cbacea2c3065}\shellfolder[attributes]
                                                 HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
   Oueries value:
cbacea2c3065}\shellfolder[callforattributes]
                                                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
   Oueries value:
cbacea2c3065}\shellfolder[restrictedattributes]
   Queries value:
                                                HKCR \verb|\wow6432| node \verb|\clsid| \{ daf 95313 - e44d - 46af - be1b - e44d - 46af - be1b - e44d - e46af - 
cbacea2c3065}\shellfolder[wantsfordisplay]
                                                 HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
   Oueries value:
cbacea2c3065}\shellfolder[hidefolderverbs]
                                                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
   Oueries value:
cbacea2c3065}\shellfolder[usedrophandler]
   Queries value:
                                                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsforparsing]
                                                HKCR\wow6432 node\clsid\{daf95313-e44d-46af-be1b-}
   Oueries value:
cbacea2c3065}\shellfolder[wantsparsedisplayname]
   Oueries value:
                                                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[queryforoverlay]
   Queries value:
                                                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[mapnetdriveverbs]
                                                 HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
   Oueries value:
cbacea2c3065}\shellfolder[queryforinfotip]
```

```
Oueries value:
                                     HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[hideinwebview]
  Oueries value:
                                     HKCR \land wow 6432 node \land clsid \land \{daf95313-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46af-be1b-e44d-46a
cbacea2c3065}\shellfolder[hideondesktopperuser]
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  Oueries value:
cbacea2c3065}\shellfolder[wantsaliasednotifications]
  Queries value:
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[nofilefolderjunction]
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  Oueries value:
cbacea2c3065}\shellfolder[pintonamespacetree]
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  Queries value:
cbacea2c3065}\shellfolder[hasnavigationenum]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{daf95313-e44d-46af-be1b-
chacea2c306511
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[attributes]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[callforattributes]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[restrictedattributes]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[wantsfordisplay]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[hidefolderverbs]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[usedrophandler]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[wantsforparsing]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[wantsparsedisplayname]
  Queries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[queryforoverlay]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[mapnetdriveverbs]
  Queries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[queryforinfotip]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[hideinwebview]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[hideondesktopperuser]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[wantsaliasednotifications]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Queries value:
4e922c26259e}\shellfolder[wantsuniversaldelegate]
  Queries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[nofilefolderiunction]
  Queries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[pintonamespacetree]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Oueries value:
4e922c26259e}\shellfolder[hasnavigationenum]
  Queries value:
4e922c26259e}]
  Oueries value:
                                     HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[attributes]
  Oueries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[callforattributes]
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
  Queries value:
96b02cfe0d52}\shellfolder[restrictedattributes]
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
  Queries value:
96b02cfe0d52}\shellfolder[wantsfordisplay]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[hidefolderverbs]
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
  Queries value:
96b02cfe0d52}\shellfolder[usedrophandler]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[wantsforparsing]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[wantsparsedisplayname]
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
  Oueries value:
96b02cfe0d52}\shellfolder[queryforoverlay]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[mapnetdriveverbs]
  Queries value:
                                     96b02cfe0d52}\shellfolder[queryforinfotip]
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
  Oueries value:
96b02cfe0d52}\shellfolder[hideinwebview]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[hideondesktopperuser]
  Queries value:
                                     HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
```

```
96b02cfe0d52}\shellfolder[wantsaliasednotifications]
                        HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
 Oueries value:
96b02cfe0d52}\shellfolder[wantsuniversaldelegate]
 Queries value:
                        HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[nofilefolderjunction]
 Queries value:
                        HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[pintonamespacetree]
 Oueries value:
                        HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[hasnavigationenum]
 Oueries value:
96b02cfe0d52}]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[attributes]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[wantsfordisplay]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[hidefolderverbs]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[usedrophandler]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[wantsforparsing]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[wantsparsedisplayname]
                        HKCR\wow6432node\clsid\f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[queryforoverlay]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[mapnetdriveverbs]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[queryforinfotip]
 Queries value:
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[hideinwebview]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[hideondesktopperuser]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Queries value:
7367fc96ef3c}\shellfolder[wantsaliasednotifications]
 Queries value:
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[wantsuniversaldelegate]
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[nofilefolderjunction]
                        HKCR\wow6432node\clsid\f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[pintonamespacetree]
 Queries value:
                        HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[hasnavigationenum]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}1
 Oueries value:
11e3-a68e-806e6f6e6963}[data]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[generation]
                        HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Oueries value:
409d6c4515e9}[drivemask]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
 Queries value:
                        \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ explorer [separate process]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
 Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Oueries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [hideicons] \end{tabular}
```

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]

 $\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]$ Oueries value:

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]

HKCR\directory[docobject] Queries value: HKCR\folder[docobject] Queries value:

HKCR\allfilesystemobjects[docobject] Queries value: HKCR\directory[browseinplace] Queries value: Queries value: HKCR\folder[browseinplace]

HKCR\allfilesystemobjects[browseinplace] Oueries value:

HKCR\directory[isshortcut] Queries value: HKCR\folder[isshortcut] Queries value:

Queries value: HKCR\allfilesystemobjects[isshortcut] HKCR\directory[alwaysshowext] Queries value:

Queries value: HKCR\directory[nevershowext] Oueries value: HKCR\folder[nevershowext]

HKCR\allfilesystemobjects[nevershowext] Queries value:

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]

Queries value: HKCR\.exe[]

Queries value: HKCR\exefile[docobject]

Oueries value: HKCR\systemfileassociations\.exe[docobject]

Queries value: HKCR\exefile[browseinplace]

Oueries value: HKCR\svstemfileassociations\.exe[browseinplace]

Oueries value: HKCR\.exe[content type] HKCR\exefile[isshortcut] Queries value:

HKCR\systemfileassociations\.exe[isshortcut] Queries value:

Queries value: HKCR\exefile[alwaysshowext]

Queries value: HKCR\systemfileassociations\.exe[alwaysshowext]

Oueries value: HKCR\exefile[nevershowext]

Queries value: HKCR\systemfileassociations\.exe[nevershowext]

db2c-424c-b029-7fe99a87c641}[category]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[name]

Oueries value:

db2c-424c-b029-7fe99a87c641}[parentfolder]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-b4bfcc3a$ db2c-424c-b029-7fe99a87c641}[description] Oueries value:

db2c-424c-b029-7fe99a87c641}[relativepath]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4bfcc3a-bc1$ db2c-424c-b029-7fe99a87c641}[parsingname] Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[infotip]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4bfcc3a-bc1$ db2c-424c-b029-7fe99a87c641}[localizedname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[icon]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b$ db2c-424c-b029-7fe99a87c641}[security]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b$ db2c-424c-b029-7fe99a87c641}[streamresource]

db2c-424c-b029-7fe99a87c641}[streamresourcetype]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ folder \ descriptions \ folder \ folde$ db2c-424c-b029-7fe99a87c641}[localredirectonly]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b$ db2c-424c-b029-7fe99a87c641}[roamable]

Queries value:

db2c-424c-b029-7fe99a87c641}[precreate]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f$ db2c-424c-b029-7fe99a87c641}[stream]

Oueries value:

db2c-424c-b029-7fe99a87c641}[publishexpandedpath]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[attributes]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[foldertypeid]

Oueries value:

db2c-424c-b029-7fe99a87c641}[initfolderhandler]

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

folders[desktop]

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value:

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Oueries value:

b8dc300d9f9d}\inprocserver32[inprocserver32]

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Queries value:

b8dc300d9f9d}\inprocserver32[]

HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Queries value:

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Oueries value:

b8dc300d9f9d}\inprocserver32[threadingmodel]

11e3-a68e-806e6f6e6963}[data]

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}[generation]

b587-4786-b4ef-bd1dc332aeae}[category]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[name]

b587-4786-b4ef-bd1dc332aeae}[parentfolder]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[description] Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[relativepath]

b587-4786-b4ef-bd1dc332aeae}[parsingname] Oueries value:

b587-4786-b4ef-bd1dc332aeae}[infotip]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[localizedname]

b587-4786-b4ef-bd1dc332aeae}[icon]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{1b3ea5dc-1explorer\} \\ folder \\ descriptions \setminus \{1b3$ b587-4786-b4ef-bd1dc332aeae}[security]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[streamresource]

b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[localredirectonly]

b587-4786-b4ef-bd1dc332aeae}[roamable]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-16der \ absolute{1} \ baselines \ absolute{1} \ baselines \ absolute{2} \ absolute{2} \ baselines \ absolute{2} \ baselines \ absolute{2} \ abs$ b587-4786-b4ef-bd1dc332aeae}[precreate]

```
Queries value:
```

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [publish expanded path]$ 

Oueries value

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [attributes]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [folder type id]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [initfolder \ handler]$ 

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]

Queries value: HKCR\exefile[nostaticdefaultverb]

Queries value: HKCR\exefile\shell[]

Queries value: HKCR\exefile\shell\open[neverdefault]

Queries value: HKCR\exefile\shell\open\command[delegateexecute]

HKCR\.asp[] Oueries value: Queries value: HKCR\.bas[] Queries value: HKCR\.bat[] HKCR\.cer[] Queries value: Queries value: HKCR\.chm[] Queries value: HKCR\.cmd[] HKCR\.com[] Oueries value: Queries value: HKCR\.cpl[] Queries value: HKCR\.crt[]

Oueries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]

Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32[threadingmodel]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[specialfolderscachesize]

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ policies \ microsoft \ windows \ current version \ internet \\$ 

settings[specialfolderscachesize]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[specialfolderscachesize]

settings[specialfolderscachesize]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature\_protocol\_lockdown[f0d96afe8a3c58bf99f8b24ff10b1a07.exe]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature\_protocol\_lockdown[\*]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\0[1806]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\0[1806]

Queries value: HKCR\exefile\shell\open\command[command]
Queries value: HKCR\exefile\shell\open\command[]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [inherit consolehandles]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[restrictrun]

Queries value:

 $\label{lower} HKLM \software \microsoft \windows \current version \policies \explorer [disallow run] \\ Queries \value: HKCR \exefile \shell \open [setworking directory from target]$ 

Queries value: HKCR\exefile\shell\open[noworkingdirectory]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

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

options[disablelocaloverride]

Queries value: HKCU\software\microsoft\visual basic\6.0[allowunsafeobjectpassing]
Queries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32[cmd]

Queries value: HKLM\software\wow6432node\microsoft\command processor[disableunccheck]
Queries value: HKLM\software\wow6432node\microsoft\command processor[enableextensions]
Queries value: HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]
Queries value: HKLM\software\wow6432node\microsoft\command processor[defaultcolor]
Queries value: HKLM\software\wow6432node\microsoft\command processor[completionchar]

Queries value: HKLM\software\wow6432node\microsoft\command

processor[pathcompletionchar]

Queries value: HKLM\software\wow6432node\microsoft\command processor[autorun]
Queries value: HKCU\software\microsoft\command processor[disableunccheck]

```
HKCU\software\microsoft\command processor[enableextensions]
  Oueries value:
  Oueries value:
                                    HKCU\software\microsoft\command processor[delayedexpansion]
  Oueries value:
                                    HKCU\software\microsoft\command processor[defaultcolor]
                                    HKCU\software\microsoft\command processor[completionchar]
  Queries value:
  Oueries value:
                                    HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value:
                                    HKCU\software\microsoft\command processor[autorun]
                                    HKLM\software\wow6432node\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[tasklist]
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Oueries value:
                                    HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
                                    HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
  Queries value:
00aa004b2e24}\inprocserver32[]
  Queries value:
                                    HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
                                   HKLM\software\wow6432node\microsoft\wbem\cimom[logging directory]
  Oueries value:
  Queries value:
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
  Queries value:
                                    HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Oueries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \
provider[image path]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:
                                    HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds]
  Queries value:
                                    HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                    HKLM\software\microsoft\cryptography[machineguid]
  Oueries value:
                                    HKCR\wow6432node\interface\{00000134-0000-0000-c000-
  Queries value:
00000000046}\proxystubclsid32[]
                                   HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:
                                    HKLM\software\microsoft\sqmclient\windows\disabledprocesses[36a1bda3]
                                    HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Oueries value:
                                    Queries value:
00c04fb68820}\proxystubclsid32[]
                                   HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
  Queries value:
                                    HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[]
                                   HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                                   HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
  Oueries value:
930efe48a887}\proxystubclsid32[]
                                    HKCR \setminus wow6432 \\ node \\ clsid \\ \{674b6698 - ee92 - 11d0 - ad71 - 00c04fd8fdff\}[]
  Queries value:
                                    HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Queries value:
00c04fd8fdff}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Queries value:
00c04fd8fdff}\inprocserver32[]
  Oueries value:
                                   HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[threadingmodel]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
  Queries value:
  Queries value:
                                    HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
                                    HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Oueries value:
  Queries value:
                                    HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32[]
  Queries value:
                                    HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
                                    HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Oueries value:
ce99a996d9ea}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Oueries value:
ce99a996d9ea}\inprocserver32[1
                                   HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Queries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                                   HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
  Oueries value:
00000000001}\proxystubclsid32[]
                                    HKCR \land wow6432 node \land \{1b1cad8c-2dab-11d2-b604-00104b703efd\}[]
  Oueries value:
  Oueries value:
                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[]
  Queries value:
                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
```

00104b703efd}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}\proxystubclsid32[]

Queries value: HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}\proxystubclsid32[]

Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}[]

Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\inprocserver32[threadingmodel]

Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[enablefiletracing]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[enableconsoletracing] Sets/Creates value:

 $\label{lem:hklmsoftwarewow6432node} HKLM\software\wow6432node\microsoft\tracing\fod96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[filetracingmask] \\ Sets/Creates\ value:$ 

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[consoletracingmask]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[maxfilesize]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasapi32[filedirectory]
Sets/Creates value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasmancs[enablefiletracing] Sets/Creates value:$ 

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasmancs[enableconsoletracing]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasmancs[filetracingmask]
Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ fod 96afe 8a 3c 58bf 99f8b 24ff 10b 1a 07\_rasmancs \ [consoletracing mask] \\ Sets \ / Creates \ value:$ 

HKLM\software\wow6432node\microsoft\tracing\f0d96afe8a3c58bf99f8b24ff10b1a07\_rasmancs[maxfilesize]
Sets/Creates value:

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyenable]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[savedlegacysettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[autodetect]