Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3326, Task ID: 811

Task ID: 811 Risk Level: 10

Date Processed: 2016-05-18 10:40:51 (UTC)

Processing Time: 11.61 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"

Sample ID: 3326 Type: basic Owner: admin

Label: 6f21fb21650da014d87426fa0bd8e7f2

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

File Type: PE32:win32:gu File Size: 177664 bytes

MD5: 6f21fb21650da014d87426fa0bd8e7f2

SHA256: 34f1a3cc2318939b243bfc434f9ecfa721574ded9a3958a970d0b817d536885f

Description: None

Pattern Matching Results

4 Terminates process under Windows subfolder

10 Creates malicious events: Beebone [Trojan]

6 Checks task list from command line

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe

["C:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"]

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

tasklist&&del 6f21fb21650da014d87426fa0bd8e7f2.exe]

Creates process: \SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe

0xffffffff]

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

Terminates process: C:\Windows\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe

Terminates process: C:\Windows\SysWOW64\tasklist.exe
Terminates process: C:\Windows\SysWOW64\cmd.exe
Terminates process: C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

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

6F21FB21650DA014D87426FA0BD8E7F2.EXE

File System Events

Creates: C:\Users\Admin

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

Creates: 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: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens: C:\Windows\Prefetch\6F21FB21650DA014D87426FA0BD8E-9A6B5DAF.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\apphelp.dll

Opens: C:\Windows\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe

Opens: C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\SysWOW64\winmm.dll C:\Windows\SysWOW64\msvbvm60.dll Opens: Opens: C:\Windows\SysWOW64\winmmbase.dll Opens: C:\Windows\SysWOW64\sechost.dll C:\Windows\SysWOW64\combase.dll Opens: C:\Windows\SysWOW64\msvcrt.dll Opens: C:\Windows\SysWOW64\gdi32.dll Opens: C:\Windows\SysWOW64\user32.dll Opens:

Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\imm32.dll

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll

```
C:\Windows\SysWOW64\cryptbase.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\sspicli.dll
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
                         C:\Windows\SysWOW64\oleaut32.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C:\Windows\SysWOW64\sxs.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\clbcatq.dll
 Opens:
                         C:\Windows\Fonts\sserife.fon
 Opens:
                         C:\Windows\SysWOW64\dwmapi.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\user32.dll.mui
 Opens:
                         C:\Windows\SysWOW64\iertutil.dll
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\Windows\SysWOW64\secur32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
                         C:\Windows\SysWOW64\SHCore.dll
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\counters.dat
 Opens:
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
                         C:\Windows\SysWOW64\nsi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
                         C:\Windows\SysWOW64\winhttp.dll
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
                         C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
 Opens:
                         C:\Windows\System32\Drivers\etc\hosts
 Opens:
                         C:\Windows\SysWOW64\propsys.dll
                         C:\Windows\SysWOW64\cfgmgr32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\devobj.dll
 Opens:
                         C:\Windows\SysWOW64\setupapi.dll
                         C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens:
 Opens:
                         4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db
 Opens:
                         C:\Windows\SysWOW64\desktop.ini
 Opens:
                         C:\Windows\SysWOW64\en-US\propsys.dll.mui
                         C:\Users\Admin\Desktop\desktop.ini
 Opens:
                         C:\Windows\SysWOW64\cmd.exe
 Opens:
 Opens:
                         C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
 Opens:
                         c:
 Opens:
                         C:\Windows\Globalization
 Opens:
                         C:\Windows\Globalization\Sorting
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\SysWOW64\wbem
 Opens:
                         C:\Windows\System32\ntdll.dll
 Opens:
                         C:\Windows\System32\wow64win.dll
 Opens:
                         C:\Windows\System32\wow64cpu.dll
 Opens:
                         C:\Windows\System32\kernel32.dll
 Opens:
                         C:\Windows\System32\user32.dll
 Opens:
                         C:\Windows\System32\locale.nls
 Opens:
                         C:\Windows\SysWOW64\wbem\WMIC.exe
 Opens:
                         C:\Windows\WINHELP.INI
                         C:\Windows\System32\conhost.exe
 Opens:
 Opens:
                         C:\Windows\System32\combase.dll
 Opens:
                         C:\Windows\System32\en-US\conhost.exe.mui
 Opens:
                         C:\Windows\System32\ole32.dll
 Opens:
                         C:\Windows\System32\uxtheme.dll
 Opens:
                         C:\Windows\System32\cmd.exe
 Opens:
                         C:\Windows\System32\en-US\cmd.exe.mui
 Opens:
                         C:\Windows\System32\dwmapi.dll
                         C:\Windows\System32\en-US\user32.dll.mui
 Opens:
 Opens:
                         C:\Windows\system32\uxtheme.dll.Config
                         C:\Windows\WinSxS\amd64_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
 Opens:
                         C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
                         C:\Windows\Svstem32\SHCore.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\tasklist.exe
```

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

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

Opens: C:\Windows\SysWOW64\en-US\tasklist.exe.mui C:\Windows\SysWOW64\en-US\KernelBase.dll.mui Opens: C:\Windows\SysWOW64\wbem\wbemprox.dll Opens:

Opens: C:\Windows\SysWOW64\wbemcomn.dll C:\Windows\SysWOW64\winsta.dll Opens: C:\Windows\SysWOW64\wbem\wbemsvc.dll Opens: C:\Windows\SysWOW64\wbem\fastprox.dll Opens: C:\Windows\SysWOW64\wbem\wmiutils.dll Opens:

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

Opens: C:\Windows\SysWOW64\en-US\cmd.exe.mui

C:\Windows\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe Reads from:

Reads from: C:\Windows\System32\Drivers\etc\hosts Reads from: C:\Users\Admin\Desktop\desktop.ini Reads from:

C:\Windows\SysWOW64\cmd.exe Reads from: C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf

Reads from: C:\Windows\SysWOW64\tasklist.exe

Network Events

DNS query: 80170.z0dns.com Sends data to: 0.0.0.0:53 Receives data from: 0.0.0.0:53

Windows Registry Events

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

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

settings\connections

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap\

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

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:

settings[autodetect]

Deletes value:

settings\zonemap[proxybypass]

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

Deletes value:

HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]

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

settings\zonemap[intranetname] HKLM\software\wow6432node\microsoft\windows\currentversion\internet

Deletes value: settings\zonemap[intranetname]

HKLM\software\microsoft\wow64 Opens kev:

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

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens kev: HKI M\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\system\currentcontrolset\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 kev: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key:

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: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side$

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

HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog Opens key:

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

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

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

execution options

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

options

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\

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

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

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

Opens key:

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

Opens key: HKLM\software\microsoft\ole

Opens key: HKLM\software\wow6432node\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\sorting\ids
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\software\policies\microsoft\sqmclient\windows

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

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

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: HKLM\software\microsoft\windowsruntime\clsid

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{85847f48-d652-4fd3-9cd1-

3ddafdba1a15}

Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15} Opens key: HKCU\software\classes\www6432node\clsid\{85847f48-d652-4fd3-9cd1-

3ddafdba1a15}

Opens key: HKCR\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}
Opens key: HKCU\software\classes\activatableclasses\clsid

3ddafdba1a15}

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{a450fe5b-6ab7-4a3c-9cf3-

3cee05d360c1}

Opens key: HKCR\activatableclasses\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}
Opens key: HKCU\software\classes\www6432node\clsid\{a450fe5b-6ab7-4a3c-9cf3-

3cee05d360c1}

 Opens key:
 HKCR\wow6432node\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}

 Opens key:
 HKCU\software\classes\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}

Opens key: HKCR\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}

Opens key: HKCU\software\classes\activatableclasses\clsid\{a450fe5b-6ab7-4a3c-9cf3-

3cee05d360c1}

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{56d37229-f433-4eef-a6a7-

b69dd0e003a3}

Opens key: HKCR\activatableclasses\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}
Opens key: HKCU\software\classes\ww6432node\clsid\{56d37229-f433-4eef-a6a7-

b69dd0e003a3}

Opens key: HKCR\wow6432node\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}

Opens key: HKCU\software\classes\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}

Opens key: HKCR\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}

Opens key: HKCU\software\classes\activatableclasses\clsid\{56d37229-f433-4eef-a6a7-

b69dd0e003a3}

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{074c6e97-3f4e-4659-9428-

62a3d81a47c1}

62a3d81a47c1}

2a3d81a4/c1}
Opens key: HKCR\wow6432node\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}

Opens key: HKCU\software\classes\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}
Opens key: HKCR\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}

Opens key: HKCU\software\classes\activatableclasses\clsid\{074c6e97-3f4e-4659-9428-

62a3d81a47c1}

62a3081a4/c1}

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{98e514e2-7646-40b7-9b56-

9292aacf45cb}

 $HKCR \land ctivatable classes \land clsid \land \{98e514e2-7646-40b7-9b56-9292 aacf45cb\}$ Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{98e514e2-7646-40b7-9b5$ Opens key: 9292aacf45cb} Opens key: HKCR\wow6432node\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb} Opens key: HKCU\software\classes\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb} Opens key: HKCR\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb} Opens key: HKCU\software\classes\activatableclasses\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb} $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{1ec267b1-9ab3-4fd2-840e-1ec267b1-9ab3-6667b1-9ab3-9ab3-6667b1-9ab3-6667b1-9ab3-6667b1-9ab3-6667b1-9ab3-6667b1-9ab3-$ Opens key: ec868c13387b} Opens key: HKCR\activatableclasses\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b} Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1ec267b1 - 9ab3 - 4fd2 - 840e - 1462 - 840e - 1462 - 840e - 1462$ ec868c13387b} HKCR\wow6432node\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b} Opens key: Opens key: HKCU\software\classes\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b} Opens key: HKCR\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b} Opens key: HKCU\software\classes\activatableclasses\clsid\{1ec267b1-9ab3-4fd2-840eec868c13387b} Opens key: 5e1ca200bf54} Opens key: HKCR\activatableclasses\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} Opens key: HKCU\software\classes\wow6432node\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} Opens key: HKCR\wow6432node\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} Opens key: HKCU\software\classes\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} HKCR\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54} Opens key: Opens key: 5e1ca200bf54} Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\system\currentcontrolset\services\disk\enum Opens key: HKLM\software\wow6432node\microsoft\rpc HKLM\software\microsoft\rpc Opens key: Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: HKLM\system\setup $HKLM \verb|\software| \verb|\wow6432| node \verb|\policies| microsoft| windows nt \verb|\rpc| rosoft| windows nt \|\rpc| rosoft| rosoft| windows nt \|\rpc| rosoft| windows nt \|\rpc| rosoft| rosoft|$ Opens key: Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: 33be-4251-ba85-6007caedcf9d} Opens key: 33be-4251-ba85-6007caedcf9d}\propertybag $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer$ Opens key: Opens key: $HKCU \ software \ `microsoft\ `windows \ `current version \ `explorer \ `session in fo' 1 \ `limits \ `limits \ `explorer' \ `session \ `info' 1 \ `limits \ `explorer' \ `session \ `explorer' \ `session \ `info' 1 \ `explorer' \ `explorer'' \ `explorer' \ `explorer' \ `explorer'' \ `explo$ Opens key: Opens key: HKU\ Opens key: HKU\.default Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\profilelist HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders $HKLM \ software \ \ wow 6432 node \ \ microsoft \ \ windows \ \ current version \ \ side by side \ \ as sembly storage roots$ Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings HKLM\software\wow6432node\policies\microsoft\internet Opens key: explorer\main\featurecontrol HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens kev: $\label{lem:hccu} \verb+KCU\+ software\+ policies\+ microsoft\+ internet\ explorer\+ main\+ feature control$ Opens key: Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol $\label{thm:linear} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main\sc microsoft\sc main\sc main\sc microsoft\sc microsoft\sc$ Opens key:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKCU\software\microsoft\internet

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_mime_handling
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
 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_bufferbreaking_818408
 Opens key:
                         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
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
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 key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet settings
                         HKLM\software\wow6432node\policies
 Opens key:
 Opens key:
                         HKCU\software\policies
 Opens key:
                         HKCU\software
                         HKLM\software\wow6432node
 Opens key:
 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
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\main
 Opens key:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
```

```
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
                      HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
 Opens key:
                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 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
 Opens key:
                      HKCU\software\microsoft\internet
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
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 Opens key:
                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 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\3b74704e
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
Opens key:
Opens key:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
                      HKLM\software\policies\microsoft\peerdist\service
 Opens kev:
 Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\peerdist\service
 Opens key:
                      HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
                      HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens kev:
                      HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                      HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens key:
                      HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
 Opens key:
                      HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key:
                      {\it HKLM \ } system \ `current control set \ `services \ 'dn scache \ 'parameters
 Opens kev:
                      HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
 Opens key:
                      HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens kev:
                      HKLM\system\currentcontrolset\services\dns
 Opens key:
                      HKLM\software\wow6432node\policies\microsoft\windows
```

 $\label{thm:local-control} \begin{tabular}{ll} HKLM \end{tabular} which is a property of the control of the co$

HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig

nt\dnsclient\dnspolicyconfig

Opens key:

Opens kev:

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

settings\5.0\cache\content

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:

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

Opens key:

Opens key:

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \windows \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current version \explorer \folder \f$

Opens key:

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

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

nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

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

1923240461-1905901954-2556564120-1001

Opens key:

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

settings\5.0\cache\cookies

Opens key:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots$

Opens key:

Opens key:

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

Opens key:

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

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

settings\5.0\cache\history

Opens key:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}}$

Opens key:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ \ property bag$

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

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

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{00000323-0000-0000-c000-

000000000046}

00000000046}

 Opens key:
 HKCR\wow6432node\clsid\{00000323-0000-0000-c000-00000000046}

 Opens key:
 HKCU\software\classes\clsid\{00000323-0000-0000-c000-000000000046}

Opens key: HKCR\clsid\{00000323-0000-0000-0000-00000000046}

Opens key: HKCU\software\classes\activatableclasses\clsid\{00000323-0000-0000-c000-

000000000046}

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCU} \\ \mathsf{software} \\ \mathsf{classes} \\ \mathsf{appid} \\ \mathsf{def21fb21650da014d87426fa0bd8e7f2.exe} \\$

Opens key: HKCR\appid\6f21fb21650da014d87426fa0bd8e7f2.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat

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

Opens key:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\cryptography\defaults\provider\microsoft\ strong\ cryptographic provider$

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

Opens key: HKLM\software\microsoft\cryptography

 $Opens\;key: \\ \qquad \qquad \mathsf{HKLM} \\ \mathsf{software} \\ \mathsf{wow} \\ \mathsf{6432} \\ \mathsf{node} \\ \mathsf{microsoft} \\ \mathsf{cryptography} \\ \mathsf{offload}$

Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-

00000000046}

000000000046}\proxystubclsid32

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

00000000046}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-

4f27df8760d0}

4f27df8760d0}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-

4f27df8760d0}\proxystubclsid32

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-

60ce2149e33c}

```
Opens key:
                                                    HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
   Opens key:
                                                    HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}
                                                    HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
   Opens key:
   Opens kev:
                                                    HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\treatas
                                                    HKCR \setminus \{057eee47-2572-4aa1-88d7-60ce2149e33c\} \setminus \{057eee47-4aa1-88d7-60ce2149e33c\} \setminus \{057eee47-4aa1-86d7-60ce2149e35c\} \setminus \{057eee47-4aa1-86d7-60ce2149e33c\} \setminus \{057eee47-4aa1-86d7-60ce2149e35c\} \setminus \{057eee47-60ce2149e35c\} \setminus \{057eee47-60ce2149e35c\} \setminus \{057eee47-60ce21466c\} \setminus \{057eee47-60ce214666c\} 
   Opens key:
   Opens key:
                                                    HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32
   Opens key:
                                                    HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32
   Opens key:
                                                    60ce2149e33c}\inprochandler32
                                                   HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
   Opens key:
60ce2149e33c}\inprochandler32
   Opens key:
                                                   HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprochandler
   Opens key:
                                                   HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprochandler
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
                                                   HKCU\software\microsoft\internet
   Opens key:
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\zonemap\ranges\
   Opens key:
                                                    HKCU\zonemap\ranges\
                                                   HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
   Opens kev:
                                                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
   Opens key:
                                                    \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap
   Opens kev:
                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
                                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\
   Opens key:
                                                    \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
settings\zonemap\
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\ranges\
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\protocoldefaults\
                                                    HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\domains\
   Opens key:
                                                    settings\zonemap\domains\
                                                    HKLM\software\policies\microsoft\internet explorer\security
   Opens key:
   Opens key:
                                                    HKCU\software\microsoft\windows\currentversion\internet settings\zones\
   Opens key:
                                                    HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
   Opens key:
                                                    HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
   Opens key:
                                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{microsoft\windows\currentversion\internet settings\zones\2}} \mbox{} \\ \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{
   Opens key:
                                                    HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
   Opens key:
                                                    HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
   Opens key:
                                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones
                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
   Opens key:
                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\0
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet_settings\zones\1
   Opens key:
                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
   Opens key:
                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
```

```
Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\2
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
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 kev:
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 kev:
explorer\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 key:
settings\lockdown_zones\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet
settings\lockdown_zones\0
                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
  Opens kev:
HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\1
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\1
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
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
                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\4
  Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\4
  Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
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
```

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$

settings\winhttp

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

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient

Opens key: HKLM\software\policies\microsoft\system\dnsclient

Opens key:

 $HKLM \ system \ current control set \ services \ troip 6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7$

55779daa70e9}

Opens key:

806e6f6e6963}

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-

806e6f6e6963}

Opens key:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{a04231f6-42eb-4732-b850-472-b850-472-b$

25b8d56dd1d8} Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-

8a6dc56e0da9}

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}

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

Opens key:

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

Opens key

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\desktop\namespace

Opens key:

7b94-4dc3-b131-e946b44c8dd5}

Opens key:

d933-450a-90e6-4acd2e9408fe}

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus desktop \setminus names pace \setminus \{11016101-101610-101$

e366-4d22-bc06-4ada335c892b}

Opens key:

a00a-44d7-9371-beb064c98683}

Opens key:

 $HKLM \label{lem:hkkm} KLM \label{lem:hkkm} HKLM \label{lem:hkkm} White \label{lem:hkkm} HKLM \label{lem:hkkm} White \label{lkkm} White \label{lkkm} White \label{lkm} White \label{lkm} White \label{lkm} Wh$

038b-4685-ab02-99bb52d3fb8b}

Opens key:

ad25-11d0-98a8-0800361b1103}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{5399e694-

6ce5-4d6c-8fce-1d8870fdcba0}

Opens key:

3f72-44a7-89c5-5595fe6b30ee}

Opens key:

5081-101b-9f08-00aa002f954e}

Opens key:

1c21-4f30-a98f-4e52906d3b56}

Opens key:

6bd1-4c86-9454-beb04e94c819}

Opens key:

 $HKLM \label{eq:hklm} KLM \label{eq:hklm} HKLM \label{eq:hklm} Software \label{eq:hklm} wow 6432 node \label{eq:hklm} icrosoft \label{eq:hklm} with the label \label{eq:hklm} With the label \label{eq:hklm} With the label \label{eq:hklm} With the label \label \l$

1c37-4a49-a12e-4b2d810d956b}

Opens key:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{le$

4fff-11e0-89e2-7b86dfd72085}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{a00ee528-

ebd9-48b8-944a-8942113d46ac}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{b4fb3f98-$

c1ea-428d-a78a-d1f5659cba93}

```
21cb-41b2-a086-b309680c6b7e}
       Opens key:
e44d-46af-be1b-cbacea2c3065}
       Opens key:
9397-435c-8f95-4e922c26259e}
       Opens key:
9ea8-4870-83b1-96b02cfe0d52}
       Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{edc 978d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-1678d6-167800-1678d6-1678d6-167800-1678d6-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-167800-1678000-1678000-167800-1678000-167800-167800-1678000-167800-167800-167800-1678000-167800-167800-16
4d53-4b2f-a265-5805674be568}
       Opens key:
be21-4350-88b0-7367fc96ef3c}
       Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace
       Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders
       Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows \ top \ names pace
       Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in foll \ desktop \ names pace \ delegate folders
       Opens key:
                                                                                                           HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
                                                                                                          HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
       Opens key:
08002b30309d}\shellfolder
                                                                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (20d04fe0-delta) + (20d04fe0-delta) +
       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 \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{208d2c60 - 3aea - 1069 - a2d7 - a2d7
       Opens key:
08002b30309d}\shellfolder
                                                                                                          HKCR\wow6432 node\clsid\{208d2c60-3aea-1069-a2d7-4c2d}
       Opens key:
 08002b30309d}\shellfolder
                                                                                                          HKCU\software\microsoft\windows\currentversion\explorer\clsid\{208d2c60-
       Opens kev:
 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 \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (871c5380-64) + (871c53
       Opens kev:
42a0-1069-a2ea-08002b30309d}\shellfolder
       Opens key:
                                                                                                          HKCU\software\classes\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder
       Opens key:
                                                                                                          HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
 00aa002f954e}\shellfolder
                                                                                                           Opens key:
5081-101b-9f08-00aa002f954e}\shellfolder
9f08-00aa002f954e}\shellfolder
                                                                                                           HKCU\software\classes\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
       Opens key:
beb064c98683}\shellfolder
       Opens key:
                                                                                                          HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder
                                                                                                          HKCU\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-
       Opens key:
 a00a-44d7-9371-beb064c98683}\shellfolder
       Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus windows \setminus current \\ version \setminus explorer \setminus (26ee 0668 - a00a - 44d7 - a00a - a
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 \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'clsid \ ' 59031a47-inches \ 'frame' \ 'f
       Opens kev:
3f72-44a7-89c5-5595fe6b30ee}\shellfolder
       Opens kev:
89c5-5595fe6b30ee}\shellfolder
       Opens key:
                                                                                                           e946b44c8dd5}\shellfolder
```

HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-

e946b44c8dd5}\shellfolder $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{031e4825-explorer\} \setminus \{031e4825-explore$ Opens key: 7b94-4dc3-b131-e946b44c8dd5}\shellfolder Opens key: b131-e946b44c8dd5}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-Opens key: 4acd2e9408fe}\shellfolder HKCU\software\microsoft\windows\currentversion\explorer\clsid\{04731b67-Opens kev: d933-450a-90e6-4acd2e9408fe}\shellfolder Opens key: 90e6-4acd2e9408fe}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder Opens key: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016101-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016100-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{11016100-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explo$ Opens key: e366-4d22-bc06-4ada335c892b}\shellfolder Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{11016101-e366-4d22bc06-4ada335c892b}\shellfolder Opens key: 99bb52d3fb8b}\shellfolder HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-Opens key: 99bb52d3fb8b}\shellfolder $HKCU \ software \ `microsoft\ `windows\ `current version\ `explorer\ `clsid\ `\{4336a54d-1646, and an additional to the control of the contr$ Opens key: 038b-4685-ab02-99bb52d3fb8b}\shellfolder Opens key: ab02-99bb52d3fb8b}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-Opens key: 0800361b1103}\shellfolder $\label{thm:local-continuous} HKCU \software \microsoft \windows \current version \explorer \clsid \classes \c$ Opens key: ad25-11d0-98a8-0800361b1103}\shellfolder Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (450d8 fba-ad25-11d0-d845) \ described \ (450d8 fba-ad25-d845) \ described \ (450d8 fba-ad2$ 98a8-0800361b1103}\shellfolder HKCU\software\classes\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-Opens kev: 1d8870fdcba0}\shellfolder HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-Opens kev: 1d8870fdcba0}\shellfolder Opens key: 6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder Opens kev: 8fce-1d8870fdcba0}\shellfolder HKCU\software\classes\wow6432node\clsid\{64693913-1c21-4f30-a98f-Opens key: 4e52906d3b56}\shellfolder HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-Opens key: 4e52906d3b56}\shellfolder Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{64693913-1c21-4f30-a98f-4e52906d3b56}\shellfolder Opens kev: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{64693913-1c21-4f30-1$ a98f-4e52906d3b56}\shellfolder Opens key: HKCU\software\classes\wow6432node\clsid\{89d83576-6bd1-4c86-9454beb04e94c819}\shellfolder HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-Opens key: beb04e94c819}\shellfolder Opens key: 6bd1-4c86-9454-beb04e94c819}\shellfolder Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (89d83576-6bd1-4c86-$ 9454-beb04e94c819}\shellfolder Opens kev: HKCU\software\classes\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-Opens kev: 4b2d810d956b}\shellfolder $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{9343812e-the clsid \setminus \{9343812e$ Opens key: 1c37-4a49-a12e-4b2d810d956b}\shellfolder Opens kev: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (9343812e-1c37-4a49-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4$ a12e-4b2d810d956b}\shellfolder HKCU\software\classes\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-Opens kev: 7b86dfd72085}\shellfolder Opens key: HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-7b86dfd72085}\shellfolder Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{98f275b4-microsoft \setminus windows \setminus current version \setminus \{98f275b4-microsoft \setminus \{98f275b4-m$

```
4fff-11e0-89e2-7b86dfd72085}\shellfolder
         Opens key:
89e2-7b86dfd72085}\shellfolder
                                                                                                                                                      HKCU\software\classes\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
         Opens kev:
  8942113d46ac}\shellfolder
                                                                                                                                                     HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
         Opens key:
  8942113d46ac}\shellfolder
                                                                                                                                                     HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{a00ee528-explorer\} \setminus \{a00ee528
          Opens key:
  ebd9-48b8-944a-8942113d46ac}\shellfolder
         Opens kev:
 HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{a00ee528-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-ebd9-48b8-e
  944a-8942113d46ac}\shellfolder
         Opens key:
                                                                                                                                                     HKCU\software\classes\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
 d1f5659cba93}\shellfolder
          Opens key:
                                                                                                                                                     HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
 d1f5659cba93}\shellfolder
          Opens key:
                                                                                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\clsid\{b4fb3f98-
 c1ea-428d-a78a-d1f5659cba93}\shellfolder
          Opens key:
 a78a-d1f5659cba93}\shellfolder
                                                                                                                                                      HKCU\software\classes\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
          Opens kev:
 b309680c6b7e}\shellfolder
                                                                                                                                                     HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
         Opens key:
 b309680c6b7e}\shellfolder
                                                                                                                                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid \setminus \{bd7a2e7b-five a content version \setminus explorer \setminus clsid 
          Opens key:
 21cb-41b2-a086-b309680c6b7e}\shellfolder
          Opens kev:
 a086-b309680c6b7e}\shellfolder
                                                                                                                                                     HKCU\software\classes\wow6432node\clsid\{daf95313-e44d-46af-be1b-
          Opens key:
  cbacea2c3065}\shellfolder
          Opens key:
                                                                                                                                                      HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  cbacea2c3065}\shellfolder
                                                                                                                                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf95
          Opens key:
 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-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-9497-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f-947-445f
 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\{edc978d6-4d53-4b2f-a265-
  5805674be568}\shellfolder
                                                                                                                                                     HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
         Opens key:
  5805674be568}\shellfolder
                                                                                                                                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \edc 978d6-part \cline{lem:hkcu} \edc 978d6-part \cline{l
          Opens key:
 4d53-4b2f-a265-5805674be568}\shellfolder
          Opens key:
a265-5805674be568}\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 \ current version \ explorer \ clsid \ \{f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c1a0d-f02c
 be21-4350-88b0-7367fc96ef3c}\shellfolder
          Opens key:
 HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{f02c1a0d-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-be21-4350-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
```

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

Opens key:

Opens key:

08002b30309d}\inprocserver32

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

Opens key:

HKLM\software\microsoft\windows\currentversion\setup Opens key: Opens key:

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-

94f2-00a0c91efb8b}

Opens key: $HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f5630d-b6bf-11d0-b6b$

94f2-00a0c91efb8b}\properties

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4cqc\} \ d5291c63-7c88-4cqc \ d5291c63$

11e3-be65-806e6f6e6963}\

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

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

HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-Opens kev:

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

HKCR\directory Opens key:

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

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

Opens key: HKCR\folder

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

HKCR\folder\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \all file system objects \shellex \classes \classes \all file system objects \shellex \classes \classes \all file system objects \shellex \classes \shellex \classes \shellex \shellex$ Opens key:

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

HKCR\directory\docobject Opens key:

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

Opens key: HKCR\folder\docobject

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

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: ${\tt HKCU \setminus software \setminus classes \setminus all filesystemobjects \setminus browsein place}$

Opens key: HKCR\allfilesystemobjects\browseinplace Opens kev: HKCU\software\classes\directorv\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: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f$

b8dc300d9f9d}

HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ b8dc300d9f9d}

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\treatas

 $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key:

b8dc300d9f9d}\inprocserver32

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key:

b8dc300d9f9d}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens kev:

b8dc300d9f9d}\inprochandler32

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key:

b8dc300d9f9d}\inprochandler32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ Opens key:

b8dc300d9f9d}\inprochandler

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens kev:

b8dc300d9f9d}\inprochandler

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\kindmap

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\kindmap

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

HKCU\software\classes\exefile Opens key:

Opens key: HKCR\exefile

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

HKCR\exefile\curver Opens key: HKCR\exefile\ Opens key:

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

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

Opens key: HKCR\exefile\docobject

HKCU\software\classes\systemfileassociations\.exe\docobject Opens kev:

Opens key: HKCR\systemfileassociations\.exe\docobject Opens key: HKCU\software\classes\exefile\browseinplace

HKCR\exefile\browseinplace Opens key:

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

Opens key: HKCR\systemfileassociations\.exe\browseinplace

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

Opens key: HKCR\exefile\clsid

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

Opens key: HKCR\systemfileassociations\.exe\clsid

Opens key:

db2c-424c-b029-7fe99a87c641}

db2c-424c-b029-7fe99a87c641}\propertybag

b587-4786-b4ef-bd1dc332aeae}

b587-4786-b4ef-bd1dc332aeae}\propertybag

HKCU\software\classes\exefile\shell

Opens key: HKCR\exefile\shell

HKCU\software\classes\exefile\shell\open Opens key:

Opens key: HKCR\exefile\shell\open

HKCR\wow6432node\clsid\{1649d1cf-deaf-4a68-abe8-Opens kev:

5c9f68572fd1}\inprocserver32

HKCR\exefile\shell\open\ Opens kev:

HKCU\software\classes\exefile\shell\open\command Opens key:

Opens key: HKCR\exefile\shell\open\command

Opens key: HKCU\software\classes\exefile\shell\open\droptarget

Opens kev: HKCR\exefile\shell\open\droptarget

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{76765b11-3f95-4af2-ac9d-46765b11-3f95-46765$

HKCR\activatableclasses\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}

ea55d8994f1a} Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9dea55d8994f1a}

Opens kev:

HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a} Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-

ea55d8994f1a}\treatas

HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-

ea55d8994f1a}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-

ea55d8994f1a}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-Opens key:

ea55d8994f1a}\inprochandler32

 $HKCR\wow6432 node\clsid\{76765b11-3f95-4af2-ac9d-4af2-$ Opens key:

ea55d8994f1a}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-Opens key:

ea55d8994f1a}\inprochandler

Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-

ea55d8994f1a}\inprochandler

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{7b8a2d94 - 0ac9 - 11d1 - 896c - 11d1 - 89$

00c04fb6bfc4}

HKCR\activatableclasses\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}

HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\treatas

HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32

HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-Opens kev:

00c04fb6bfc4}\inprocserver32

```
HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens key:
00c04fb6bfc4}\inprochandler32
                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens key:
00c04fb6bfc4}\inprochandler32
                         HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens kev:
00c04fb6bfc4}\inprochandler
                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Opens key:
00c04fb6bfc4}\inprochandler
 Opens key:
                         HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610 HKLM\software\wow6432node\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000 HKCU\software\microsoft\internet

Opens kev: explorer\main\featurecontrol\feature_protocol_lockdown

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

explorer\main\featurecontrol\feature_protocol_lockdown

Opens key:

settings\zones\0

Opens kev: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\

Opens key:

HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8

 $HKLM \setminus software \setminus microsoft \setminus telemetry client \setminus throttlestore \setminus sqm \setminus windows$ Opens key:

Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm Opens key: HKLM\software\microsoft\telemetryclient\throttlestore

Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8

Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows

Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm

Opens key:

 $HKLM \verb|\software\microsoft| telemetry client \verb|\throttlestore\sqm\windows\winsqm8\13238528$

Opens key:

HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528

 $HKLM \setminus software \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus telemetry client \setminus throttle store \setminus sqm \setminus irrosoft \setminus throttle store \setminus sqm \setminus irrosoft \setminus throttle store \setminus sqm \setminus irrosoft \setminus sqm \setminus s$

Opens key:

HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784

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

HKCR\exefile\progid Opens key:

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ progids \ exefile$

 ${\tt HKCU \setminus software \setminus classes \setminus exefile \setminus shell \setminus open \setminus ddeexec}$ Opens key:

Opens key: HKCR\exefile\shell\open\ddeexec

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

options\cmd.exe

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens kev: Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat

Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows nt\currentversion $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\windows}\ nt\current version\app compatflags\layers}$ Opens key:

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

nt\currentversion\appcompatflags

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

nt\currentversion\appcompatflags\custom\cmd.exe

HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

Opens key: HKCU\software\classes\applications\cmd.exe

Opens key: HKCR\applications\cmd.exe

Opens key: HKCU\software\microsoft\windows\shell\associations HKLM\software\wow6432node\microsoft\windows Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows\html help

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

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

options\conhost.exe

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

HKLM\software\microsoft\windows nt\currentversion\windows Opens kev:

HKLM\software\microsoft\oleaut Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\console\truetypefont Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen

Opens key: HKCU\console Opens key: HKCU\console\

HKCU\console\%systemroot%_system32_cmd.exe Opens key: Opens key: HKCU\console\%systemroot%\system32\cmd.exe Opens key: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange

Opens key: HKLM\software\microsoft\ctf\compatibility\conhost.exe Opens kev: HKLM\software\microsoft\windows\windows error reporting\wmr

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKCU\software\policies\microsoft\windows\system HKLM\software\wow6432node\microsoft\command processor Opens key:

Opens key: HKCU\software\microsoft\command processor

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

options\tasklist.exe

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

nt\currentversion\appcompatflags\custom\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

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

Opens key: HKCU\software\classes\appid\tasklist.exe

Opens key: HKCR\appid\tasklist.exe

Opens key:

00aa004b2e24}

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

Opens key:

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

Opens key:

 $HKCR \ wow 6432 node \ clsid \ \{4590f811-1d3a-11d0-891f-00aa 004b2e24\} \ treat as$ Opens key:

00aa004b2e24}\inprocserver32

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

00aa004b2e24}\inprocserver32

Opens key:

00aa004b2e24}\inprochandler32

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

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:

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}

HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key:

HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas

Opens key:

 $HKCR \\ wow 6432 \\ node \\ clsid \\ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \\ \\ treat \\ as \\ node \\ node$ Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

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

00c04fb68820}\inprocserver32

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

00c04fb68820}\inprochandler32

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

00c04fb68820}\inprochandler32

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

00c04fb68820}\inprochandler

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

00c04fb68820}\inprochandler

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

00c04fb68820}

Opens key: $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{f309 \\ ad18 - d86 \\ a-11 \\ d0-a075-00 \\ c04 \\ fb68820\}$ Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-

00c04fb68820}\proxystubclsid32

Opens key:

00c04fb68820}\proxystubclsid32

HKLM\software\microsoft\windowsruntime\clsid\{7c857801-7381-11cf-884d-Opens kev:

00aa004b2e24}

Opens key:

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

> HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-1464\} \\ + 11cf-884d-1464 \\ +$

Opens kev:

00aa004b2e24}\treatas HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas Opens kev:

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

00aa004b2e24}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprocserver32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{7c857801 - 7381 - 11cf - 884d - 11cf - 884d$ 00aa004b2e24}\inprochandler32 Opens key HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler Opens key: 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 Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{674b6698 - ee92 - 11d0 - ad71 - ad$ 00c04fd8fdff} HKCR\activatableclasses\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler Opens key HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-Opens key: 00aa003240c7} Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32 Opens key: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32 HKLM\software\microsoft\windowsruntime\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea} HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea} Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\treatas HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprochandler32 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea}\inprochandler32 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{d68af00a-29cb-43fa-8504-468af00a-29cb-436af00a-29$ Opens key: ce99a996d9ea}\inprochandler $HKCR\wow6432 node\clsid\{d68af00a-29cb-43fa-8504-468af00a-29cb-436af00a-29cb$ Opens key: ce99a996d9ea}\inprochandler Opens kev: HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} HKCR\activatableclasses\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens key: HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens kev: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\treatas HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\treatas Opens kev: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens kev: 252725d697ca}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler32 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens key:

252725d697ca}\inprochandler
Opens key: HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-

HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-

252725d697ca}\inprochandler32

```
252725d697ca}\inprochandler
```

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

00000000001}

Opens key: HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-00000000001)}
Opens key: HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-

000000000001}\proxystubclsid32

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}

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

00104b703efd}

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

00104b703efd}\treatas

Opens key: $\begin{tabular}{ll} HKCR\wow6432node\clsid\floates-2dab-11d2-b604-00104b703efd\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\floates-2dab-11d2-b604- \\ \end{tabular}$

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}

 Opens key:
 HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

00104b703efd}\proxystubclsid32

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-b604-00104b703efd}

00104b703efd}\proxystubclsid32

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

00104b703efd}\proxystubclsid32

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820} Opens key:

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

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

Queries value:

Queries value:

 $\label{lem:hklm} \verb|HKLM\| system\| current controls et \verb|\control\| nls \| language [install language fall back] |$

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

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

us[alternatecodepage]

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ described \ for the side by \ describe$

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

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

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.dll1

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

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrol\set\control\lsa\fipsalgorithmpolicy[enabled]

HKLM\software\wow6432node\microsoft\windows

Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]

Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]

Queries value: HKLM\system\currentcontrol\set\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrol\set\control\nls\sorting\versions[000602xx]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
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]

Oueries value:

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

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

manager[safeprocesssearchmode]

 Queries value:
 HKLM\system\currentcontrol\set\control\nls\codepage[932]

 Queries value:
 HKLM\system\currentcontrolset\control\nls\codepage[949]

 Queries value:
 HKLM\system\currentcontrolset\control\nls\codepage[950]

 Queries value:
 HKLM\system\currentcontrolset\control\nls\codepage[936]

Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[maxxxshashcount]

Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]

Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]

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

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

 Queries value:
 HKLM\system\setup[oobeinprogress]

 Queries value:
 HKLM\system\setup[systemsetupinprogress]

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

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

settings[syncmode5]

 $Queries\ value: \\ HKLM\ software\ wow 6432 node\ microsoft\ windows\ current version\ internet$

 $settings \verb|\|5.0\>| cache[sessions tart time default deltasecs]$

Queries value:

 $\label{thm:local-base-equal} HKLM \software \wow 6432 node \mbox{352481e8-33be-4251-ba85-6007} caed cf9d \category \]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [name]$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [description]$

Queries value:

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

Queries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ f9d \ [stream resource type]$

```
33be-4251-ba85-6007caedcf9d}[localredirectonly]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[roamable]
 Queries value:
33be-4251-ba85-6007caedcf9d}[precreate]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[stream]
 Queries value:
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
33be-4251-ba85-6007caedcf9d}[attributes]
 Queries value:
33be-4251-ba85-6007caedcf9d}[foldertypeid]
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
                       HKU\.default\software\microsoft\windows\currentversion\explorer\user
 Queries value:
shell folders[cache]
 Queries value:
                       HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsapiforcrack]
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[security_hklm_only]
                       HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[6f21fb21650da014d87426fa0bd8e7f2.exe]
 Queries value:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
                       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:
                       HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_mime\_handling[6f21fb21650da014d87426fa0bd8e7f2.exe]|
                       HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mime_handling[*]
                       HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature disable unicode handle closing callback[6f21fb21650da014d87426fa0bd8e7f2.exe]
 Queries value:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[fromcachetimeout]
                       \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[secureprotocols]
 Queries value:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[certificaterevocation]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[idnenabled]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[preconnectlimit]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[preresolvelimit]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sqmhttpstreamrandomuploadpoolsize]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
 Queries value:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_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[enablehttp1_1]
 Queries value:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                       HKCU\software\policies\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[proxyhttp1.1]
```

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

```
settings[enablenegotiate]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
 Oueries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxv]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirvtimesecs]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
```

```
Oueries 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]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                        Queries value:
settings[bypasssslnocachecheck]
                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttptrace]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
                        Queries value:
settings[nocheckautodialoverride]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
                        HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[dontusednsloadbalancing]
                        Queries value:
settings[sharecredswithwinhttp]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                        \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[headerexclusionlistforcache]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                        \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[warnonzonecrossing]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertrecving]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[alwaysdrainonredirect]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
 Queries value:
                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000005 \ [packed catalog item]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
 Queries 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]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[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\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries 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\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Oueries 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]
- 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\000000000003[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo]
- 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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
- 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\00000000004[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000005 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005[supportednamespace]
 Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws2_32 numhandle buckets]$

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

settings[proxysettingsperuser]

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

settings[badproxyexpirestime]
Oueries value: HKCU

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

settings[disablebranchcache]

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

settings[usefirstavailable]

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

settings[combinefalsestartdata]

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

settings[disablefalsestartblacklist]

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

settings[enforcep3pvalidity]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\peerdist\service[enable]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} = \{ param$

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [max sock addrlength]$

Queries value:

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

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings[autodetect]

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

settings\connections[savedlegacysettings]
 Queries value: HKCU\software\mi

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

Settings\connections[defaultconnectionsetting

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]

Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [usedomain name devolution]$

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns secure name query fall back]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] ${\tt HKLM \ } system \verb| current control set \verb| services \verb| dns cache \verb| parameters [use hosts file]|$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]

HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]

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

Oueries value:

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
    Queries 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:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
    Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts endermax time out]
                                                                HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
    Queries value:
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
    Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters \texttt{[resolverregistration]}
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Oueries value:
HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[name]
    Oueries value:
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[description]
    Queries value:
6fba-4fcf-9d55-7b8e7f157091}[relativepath]
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f1b32785-1000\} \\ folder \\ descriptions \setminus \{f1b3275-1000\} \\ folder \\ descriptions \setminus \{f1b3275-10000\} \\ folder \\ descriptions \setminus \{f1b3275-10000\} \\ folder \\ descriptions \setminus \{f1b3275-100000\} \\
6fba-4fcf-9d55-7b8e7f157091}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[infotip]
HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localizedname]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785-b2785
6fba-4fcf-9d55-7b8e7f157091}[icon]
    Oueries value:
6fba-4fcf-9d55-7b8e7f157091}[security]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f 1b32785-b12785 \ \ description \ \ descriptio
```

6fba-4fcf-9d55-7b8e7f157091}[streamresource]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[roamable]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[precreate]

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f 1b 32785 - 1b 32785$ 6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b2785-b27864, \ b27864, \ b$ 6fba-4fcf-9d55-7b8e7f157091}[attributes]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b2785-b27864, \ b27864, \ b$ 6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]

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

folders[local appdata]

Queries value:

0e22-4760-9afe-ea3317b67173}[category]

0e22-4760-9afe-ea3317b67173}[name]

0e22-4760-9afe-ea3317b67173}[parentfolder]

0e22-4760-9afe-ea3317b67173}[description]

0e22-4760-9afe-ea3317b67173}[relativepath]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ descriptions \setminus \{5e6c85microsoft \setminus windows \setminus current \\ descriptions \setminus$ 0e22-4760-9afe-ea3317b67173}[parsingname]

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

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]

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

Oueries value:

0e22-4760-9afe-ea3317b67173}[security]

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

0e22-4760-9afe-ea3317b67173}[streamresourcetype]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-6e8566f-6e85666f-6e85666f-6e85666f-6e8566f-6e85666f-6e8566f-6e8566f-6e85666f-6e85666f-6e85666f-6e85666f-6e85666f-6e85666$ 0e22-4760-9afe-ea3317b67173}[localredirectonly]

Queries value:

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

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

Queries value:

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

0e22-4760-9afe-ea3317b67173}[publishexpandedpath]

Queries value:

0e22-4760-9afe-ea3317b67173}[attributes]

Oueries value:

0e22-4760-9afe-ea3317b67173}[foldertypeid]

0e22-4760-9afe-ea3317b67173}[initfolderhandler]

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

1923240461-1905901954-2556564120-1001[profileimagepath]

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

settings\5.0\cache\content[cachelimit]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $HKLM \label{lem:hklm} White the latest and the la$ c0e9-4171-908e-08a611b84ff6}[localredirectonly]

Queries value:

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

Queries value:

 $HKLM \label{lem:hklm} Which was the statement of the second of the sec$ c0e9-4171-908e-08a611b84ff6}[precreate]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

folders[cookies]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

Queries value: folders[appdata]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]

Queries value:

 $\label{thm:hklm} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(d9dc8a3b-b784-432e-a781-5a1130a75963)\category\cite{Abstraction} and the second sec$

Oueries value:

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

Queries value

 $\label{thm:hklm} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(d9dc8a3b-b784-432e-a781-5a1130a75963)\cite{thm:hklm}\cite{thm:h$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[description]}$

Queries value:

Queries value:

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

Queries value

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[infotip]} \\$

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[localized name]}$

Queries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963\}[icon]$

Queries value:

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

Oueries value:

Oueries value

 $\label{limits} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions \eqref{d9dc8a3b-b784-432e-a781-5a1130a75963} [stream resource type]$

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3bb784-432e-a781-5a1130a75963\} \ [precreate]$

Oueries value:

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

Oueries value:

 $\label{thm:local-bound} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\ [publish expanded path]$

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[history]

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

settings\5.0\cache\history[cachelimit]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]

Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]

Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]

Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

Queries value:

 $\label{lem:hklmlsoftware} HKLM\software\wow6432 node\microsoft\cryptography\defaults\provider\microsoft\ strong\ cryptographic provider\[type]$

Queries value:

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

Queries value:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} policies \end{tabular} icrosoft \end{tabular} represents the constraint of the constrain$

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

000000000046}\proxystubclsid32[]

Queries value: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-

4f27df8760d0}\proxystubclsid32[]

Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]

Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-

60ce2149e33c}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-

60ce2149e33c}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-

60ce2149e33c}\inprocserver32[threadingmodel]

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[local appdata]

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

explorer\security[disablesecuritysettingscheck]

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

settings\zones\0[flags]
 Oueries value:

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

settings\zones\1[flags]

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

settings\zones\2[flags]
Queries value:

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

settings\zones\3[flags]

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

settings\zones\4[flags]

Queries value: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_local machine_lock down[6f21fb21650da014d87426fa0bd8e7f2.exe]|$

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]

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

explorer\main\featurecontrol\feature_localmachine_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]

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

explorer\main\featurecontrol\feature_localmachine_lockdown[*]

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

settings[createuricachesize] HKCU\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[createuricachesize] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] Queries value: settings[createuricachesize] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode] 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[enablepunycode] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoproxydetecttype] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\winhttp[disablebranchcache] Queries value: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[winhttplowercasehost] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a10] HKLM\system\currentcontrolset\services\winsock\setup Queries value: migration\providers\tcpip[winsock 2.0 provider id] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist] Queries value: 806e6f6e6963}[enabledhcp] Queries value: 55779daa70e9}[registrationenabled] Queries value: 55779daa70e9}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain] Oueries value: $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8$ 55779daa70e9}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver] Queries value: 55779daa70e9}[nameserver] Oueries value: 55779daa70e9}[dhcpnameserver] Queries value: 806e6f6e6963}[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[nameserver] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-be12e1de57-d6fa-11e1-be12e1de57-d6fa-10de57-d6fa-10de57-d6fa-10de57-d6fa-10de57-d6fa-10de57-d6fa-10de57-d6fa-10de57-d6fa-10de57-d6$

806e6f6e6963}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast] Queries value: 806e6f6e6963}[queryadaptername] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disabledynamicupdate]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enableadapterdomainnameregistration]

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount]

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[maxnumberofaddressestoregister]

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast]

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

Oueries value:

 $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer[maximize apps]$ Oueries value:

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

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

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

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

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [noset folders]$ Queries value:

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

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

7b94-4dc3-b131-e946b44c8dd5}[suppressionpolicy]

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

e366-4d22-bc06-4ada335c892b}[suppressionpolicy]

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

Queries value:

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

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

Queries value:

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

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

Queries value:

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

```
Oueries value:
1c21-4f30-a98f-4e52906d3b56}[suppressionpolicy]
6bd1-4c86-9454-beb04e94c819}[suppressionpolicy]
     Oueries value:
1c37-4a49-a12e-4b2d810d956b}[suppressionpolicy]
4fff-11e0-89e2-7b86dfd72085}[suppressionpolicy]
     Oueries value:
ebd9-48b8-944a-8942113d46ac}[suppressionpolicy]
     Oueries value:
c1ea-428d-a78a-d1f5659cba93}[suppressionpolicy]
     Oueries value:
HKLM \label{lem:hkkm} Lose the label of the label la
21cb-41b2-a086-b309680c6b7e}[suppressionpolicy]
     Oueries value:
\label{thm:local_continuous} \label{thm:local_continuous} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \desktop \namespace \{daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf95313-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-daf9531-d
 e44d-46af-be1b-cbacea2c3065}[suppressionpolicy]
     Oueries value:
9397-435c-8f95-4e922c26259e}[suppressionpolicy]
     Queries value:
9ea8-4870-83b1-96b02cfe0d52}[suppressionpolicy]
    Oueries value:
4d53-4b2f-a265-5805674be568}[suppressionpolicy]
     Queries value:
be21-4350-88b0-7367fc96ef3c}[suppressionpolicy]
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
 08002b30309d}\shellfolder[attributes]
                                                                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d}\shellfolder[callforattributes]
                                                                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
 08002b30309d}\shellfolder[restrictedattributes]
                                                                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
 08002b30309d}\shellfolder[foldervalueflags]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum [\{20d04fe0-3aea-1069-a2d8-microsoft \setminus current version \setminus policies \setminus polic
08002b30309d}]
     Queries value:
                                                                         HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
 08002b30309d}\shellfolder[attributes]
     Queries value:
                                                                         HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
 08002b30309d}\shellfolder[callforattributes]
     Oueries value:
                                                                         HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[restrictedattributes]
     Queries value:
                                                                        HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
 08002b30309d}\shellfolder[foldervalueflags]
     Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{208d2c60-3aea-1069-a2d7-
08002b30309d}1
                                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
     Oueries value:
 08002b30309d}\shellfolder[attributes]
    Queries value:
                                                                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 08002b30309d}\shellfolder[callforattributes]
                                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
     Queries value:
08002b30309d}\shellfolder[restrictedattributes]
                                                                         HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
     Oueries value:
08002b30309d}\shellfolder[foldervalueflags]
    Queries value:
                                                                         42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
     Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}1
                                                                         HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
     Oueries value:
00aa002f954e}\shellfolder[attributes]
     Queries value:
                                                                         HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
 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[foldervalueflags]
     Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ monenum \ [\{645ff040-5081-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-101b-9f08-1000-1000
00aa002f954e}1
```

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[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{26ee0668-a00a-44d7-9371-
beb064c98683}]
                         HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Oueries value:
5595fe6b30ee}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Queries value:
5595fe6b30ee}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Queries value:
5595fe6b30ee}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Oueries value:
5595fe6b30ee}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-
5595fe6b30ee}]
 Queries value:
                          HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Queries value:
e946b44c8dd5}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{031e4825-7b94-4dc3-b131-
e946b44c8dd5}1
                          HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Queries value:
4acd2e9408fe}\shellfolder[attributes]
 Oueries value:
                         HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[restrictedattributes]
                          HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Queries value:
4acd2e9408fe}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{04731b67-d933-450a-90e6-
4acd2e9408fe}1
                         HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
 Queries value:
4ada335c892b}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
 Queries value:
4ada335c892b}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
 Queries value:
4ada335c892b}\shellfolder[restrictedattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{11016101-e366-4d22-bc06-
4ada335c892b}1
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
 Oueries value:
99bb52d3fb8b}\shellfolder[attributes]
 Oueries value:
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
 Oueries value:
99bb52d3fb8b}\shellfolder[restrictedattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{4336a54d-038b-4685-ab02-
99bb52d3fb8b}1
                          HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
 Oueries value:
0800361b1103}\shellfolder[attributes]
 Queries value:
                         HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
 Oueries value:
0800361b1103}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
 Oueries value:
0800361b1103}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{450d8fba-ad25-11d0-98a8-
0800361b1103}1
 Queries value:
                         HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
 Oueries value:
1d8870fdcba0}\shellfolder[callforattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[restrictedattributes]
 Queries value:
                          HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
```

```
1d8870fdcba0}\shellfolder[foldervalueflags]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}1
                                                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
   Oueries value:
4e52906d3b56}\shellfolder[attributes]
   Queries value:
                                                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder[callforattributes]
                                                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
   Queries value:
4e52906d3b56}\shellfolder[restrictedattributes]
                                                 HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
   Oueries value:
4e52906d3b56}\shellfolder[foldervalueflags]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{64693913-1c21-4f30-a98f-
4e52906d3b56}]
   Queries value:
                                                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[attributes]
                                                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Queries value:
beb04e94c819}\shellfolder[callforattributes]
                                                 HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Queries value:
beb04e94c819}\shellfolder[restrictedattributes]
                                                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
   Queries value:
beb04e94c819}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{89d83576-6bd1-4c86-9454-
beb04e94c819}1
                                                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Queries value:
4b2d810d956b}\shellfolder[attributes]
                                                  HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{9343812 \\ e-1c37-4a49-a12 \\ e-
   Oueries value:
4b2d810d956b}\shellfolder[callforattributes]
                                                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
   Oueries value:
4b2d810d956b}\shellfolder[restrictedattributes]
                                                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[foldervalueflags]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9343812e-1c37-4a49-a12e-
4b2d810d956b}1
                                                  HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
   Queries value:
7b86dfd72085}\shellfolder[attributes]
                                                  HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
   Queries value:
7b86dfd72085}\shellfolder[callforattributes]
                                                 HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
   Queries value:
7b86dfd72085}\shellfolder[restrictedattributes]
   Queries value:
                                                 HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder[foldervalueflags]
   Queries value:
7b86dfd72085}1
                                                  HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
   Oueries value:
8942113d46ac}\shellfolder[attributes]
   Oueries value:
                                                  HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[callforattributes]
   Queries value:
                                                  HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[restrictedattributes]
                                                  Oueries value:
8942113d46ac}\shellfolder[foldervalueflags]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{a00ee528-ebd9-48b8-944a-
8942113d46ac}1
                                                  HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Queries value:
d1f5659cba93}\shellfolder[attributes]
                                                 Queries value:
d1f5659cba93}\shellfolder[callforattributes]
                                                  HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Oueries value:
d1f5659cba93}\shellfolder[restrictedattributes]
                                                  HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
   Oueries value:
d1f5659cba93}\shellfolder[foldervalueflags]
   Queries value:
d1f5659cba93}1
   Queries value:
                                                  HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[attributes]
                                                 HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Oueries value:
b309680c6b7e}\shellfolder[callforattributes]
                                                 HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
   Queries value:
b309680c6b7e}\shellfolder[restrictedattributes]
   Queries value:
                                                  HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[foldervalueflags]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}]
                                                  HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{daf95313 - e44d - 46af - be1b - e44d - e46af - e4
   Oueries value:
cbacea2c3065}\shellfolder[attributes]
```

```
Oueries value:
                       HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[callforattributes]
 Oueries value:
                       HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[restrictedattributes]
                       HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
 Oueries value:
cbacea2c3065}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{daf95313-e44d-46af-be1b-
cbacea2c3065}]
 Queries value:
                       HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[attributes]
                       HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
 Queries value:
4e922c26259e}\shellfolder[callforattributes]
                       HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
 Oueries value:
4e922c26259e}\shellfolder[restrictedattributes]
                       HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
 Queries value:
4e922c26259e}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{e345f35f-9397-435c-8f95-
4e922c26259e}1
                       HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
 Queries value:
96b02cfe0d52}\shellfolder[attributes]
                       HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
 Oueries value:
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[foldervalueflags]
 Oueries value:
96b02cfe0d52}1
                       HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
 Queries value:
5805674be568}\shellfolder[attributes]
 Queries value:
                       HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder[callforattributes]
                       HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
 Queries value:
5805674be568}\shellfolder[restrictedattributes]
                       Queries value:
5805674be568}\shellfolder[foldervalueflags]
 Queries value:
5805674be568}1
                       HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[attributes]
                       HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[callforattributes]
 Queries value:
                       HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[restrictedattributes]
                       HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
 Oueries value:
7367fc96ef3c}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}]
 Queries value:
                       HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
 Queries value:
11e3-be65-806e6f6e6963}[data]
 Oueries value:
11e3-be65-806e6f6e6963}[generation]
 Queries value:
                       HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
                       HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version[device path]|
 Queries value:
 Oueries value:
                       HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[data]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Queries value:
11e3-be65-806e6f6e6963}[generation]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Queries value:
                       \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[hidden]| \\ \end{tabular}
```

```
Oueries 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:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Queries value:
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced \ [autocheck select]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
  Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [shows tatus bar]
                                   HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
  Queries value:
97a27216f98a}\inprocserver32[]
                                   HKCR\directory[docobject]
  Queries value:
                                   HKCR\folder[docobject]
  Queries value:
  Queries value:
                                   HKCR\allfilesystemobjects[docobject]
  Oueries value:
                                   HKCR\directory[browseinplace]
                                   HKCR\folder[browseinplace]
  Queries value:
                                   HKCR\allfilesystemobjects[browseinplace]
  Oueries value:
  Oueries value:
                                   HKCR\directory[isshortcut]
                                   HKCR\folder[isshortcut]
  Queries value:
                                   HKCR\allfilesystemobjects[isshortcut]
  Queries value:
  Oueries value:
                                   HKCR\directory[alwaysshowext]
                                   HKCR\directory[nevershowext]
  Queries value:
  Oueries value:
                                   HKCR\folder[nevershowext]
  Oueries value:
                                   HKCR\allfilesystemobjects[nevershowext]
                                   HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
  Oueries value:
a6bb2164fbd0}\inprocserver32[]
  Queries value:
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Queries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
  Queries value:
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidiunctions]
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]
                                   HKCR\.exe[content type]
  Queries value:
                                   HKCR\.exe[]
  Oueries value:
                                   HKCR\exefile[docobject]
  Oueries value:
                                   HKCR\systemfileassociations\.exe[docobject]
  Queries value:
  Queries value:
                                   HKCR\exefile[browseinplace]
  Oueries value:
                                   HKCR\systemfileassociations\.exe[browseinplace]
                                   HKCR\exefile[isshortcut]
  Queries value:
                                   HKCR\systemfileassociations\.exe[isshortcut]
  Oueries value:
  Queries value:
                                   HKCR\exefile[alwaysshowext]
  Oueries value:
                                   HKCR\systemfileassociations\.exe[alwaysshowext]
  Queries value:
                                   HKCR\exefile[nevershowext]
  Queries value:
                                   HKCR\systemfileassociations\.exe[nevershowext]
db2c-424c-b029-7fe99a87c641}[category]
db2c-424c-b029-7fe99a87c641}[name]
  Queries value:
db2c-424c-b029-7fe99a87c641}[parentfolder]
db2c-424c-b029-7fe99a87c641}[description]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4
```

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

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

folders[desktop]

Queries value:

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

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

b587-4786-b4ef-bd1dc332aeae}[parentfolder]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[description]

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

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

b587-4786-b4ef-bd1dc332aeae}[infotip]

Queries value:

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

b587-4786-b4ef-bd1dc332aeae}[icon]

Queries value:

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

b587-4786-b4ef-bd1dc332aeae}[streamresource]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-1b4ea5dc-1$ b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[localredirectonly]

b587-4786-b4ef-bd1dc332aeae}[roamable]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[precreate]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[stream]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[attributes]

Oueries value:

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

Queries value:

b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]

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

folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]

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

HKCR\wow6432node\clsid\{1649d1cf-deaf-4a68-abe8-Queries value:

5c9f68572fd1}\inprocserver32[]

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

HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[] Queries value:

Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-

ea55d8994f1a}\inprocserver32[inprocserver32]

HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-Queries value:

ea55d8994f1a}\inprocserver32[]

HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-Queries value:

ea55d8994f1a}\inprocserver32[threadingmodel]

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

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

00c04fb6bfc4}\inprocserver32[inprocserver32]

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

00c04fb6bfc4}\inprocserver32[]

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

00c04fb6bfc4}\inprocserver32[threadingmodel]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[specialfolderscachesize]

Oueries value:

HKCU\software\policies\microsoft\windows\currentversion\internet settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[specialfolderscachesize]

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

explorer\main\featurecontrol\feature_protocol_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]

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

explorer\main\featurecontrol\feature_protocol_lockdown[*]

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

settings\zones\0[1806]

Queries value: settings\zones\0[1806]

HKLM\software\microsoft\sqmclient\windows\disabledprocesses[f189f4ab] Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\internet

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

Queries value: HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]

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

Queries value:

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

Oueries value:

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

HKLM\software\microsoft\windows\currentversion\policies\explorer[disallowrun] Queries value: HKCR\exefile\shell\open[setworkingdirectoryfromtarget]

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

Oueries value:

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

folders[cache]

Queries value: HKCR\applications\cmd.exe[immersivebroker]

Queries value: HKCU\software\microsoft\windows\shell\associations[showtoast] Oueries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]

```
HKLM \verb|\software\microsoft\windows \verb|\currentversion\side| preferex ternal manifest| \\
                          HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[conhost]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\windows[loadappinit dlls]
 Queries value:
                          HKCU\console[screencolors]
 Oueries value:
                           HKCU\console[popupcolors]
 Oueries value:
                           HKCU\console[insertmode]
 Oueries value:
                           HKCU\console[quickedit]
 Oueries value:
                           HKCU\console[codepage]
                           HKCU\console[screenbuffersize]
 Oueries value:
 Queries value:
                           HKCU\console[windowsize]
 Oueries value:
                           HKCU\console[windowposition]
 Oueries value:
                           HKCU\console[fontsize]
 Queries value:
                           HKCU\console[fontfamily]
 Oueries value:
                           HKCU\console[fontweight]
 Queries value:
                           HKCU\console[facename]
 Queries value:
                           HKCU\console[cursorsize]
 Oueries value:
                           HKCU\console[historybuffersize]
 Oueries value:
                           HKCU\console[numberofhistorybuffers]
 Queries value:
                           HKCU\console[historynodup]
 Queries value:
                           HKCU\console[colortable00]
 Queries value:
                           HKCU\console[colortable01]
 Queries value:
                           HKCU\console[colortable02]
 Queries value:
                           HKCU\console[colortable03]
                           HKCU\console[colortable041
 Oueries value:
 Queries value:
                           HKCU\console[colortable05]
 Queries value:
                           HKCU\console[colortable06]
                           HKCU\console[colortable07]
 Oueries value:
 Queries value:
                           HKCU\console[colortable08]
 Queries value:
                           HKCU\console[colortable09]
 Oueries value:
                           HKCU\console[colortable10]
                           HKCU\console[colortable11]
 Queries value:
 Queries value:
                           HKCU\console[colortable12]
 Oueries value:
                           HKCU\console[colortable13]
                           HKCU\console[colortable14]
 Queries value:
                           HKCU\console[colortable15]
 Oueries value:
 Oueries value:
                           HKCU\console[loadconime]
                           HKCU\console[extendededitkey]
 Queries value:
                           HKCU\console[extendededitkeycustom]
 Queries value:
 Oueries value:
                           HKCU\console[worddelimiters]
                           HKCU\console[trimleadingzeros]
 Queries value:
                           HKCU\console[enablecolorselection]
 Oueries value:
 Oueries value:
                           HKCU\console[scrollscale]
                           HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
 Oueries value:
                           HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
 Queries value:
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
                           HKLM\software\wow6432node\microsoft\command processor[disableunccheck]
 Oueries value:
 Oueries value:
                           HKLM\software\wow6432node\microsoft\command processor[enableextensions]
                           HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]
 Oueries value:
                           HKLM\software\wow6432node\microsoft\command processor[defaultcolor]
 Oueries value:
 Oueries value:
                           HKLM\software\wow6432node\microsoft\command processor[completionchar]
 Queries value:
                           HKLM \verb|\software\\ \verb|\wow6432| node\\ \verb|\microsoft\\ \verb|\command|
processor[pathcompletionchar]
 Queries value:
                           HKLM\software\wow6432node\microsoft\command processor[autorun]
 Oueries value:
                           HKCU\software\microsoft\command processor[disableunccheck]
                           HKCU\software\microsoft\command processor[enableextensions]
 Oueries value:
 Oueries value:
                           HKCU\software\microsoft\command processor[delayedexpansion]
                           HKCU\software\microsoft\command processor[defaultcolor]
 Queries value:
 Queries value:
                           HKCU\software\microsoft\command processor[completionchar]
 Oueries value:
                           \label{local-equation} \mbox{HKCU\software\mbox{\sc microsoft\command processor[pathcompletionchar]}}
                           HKCU\software\microsoft\command processor[autorun]
 Queries value:
 Oueries value:
                           HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[tasklist]
                           HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
 Queries value:
                           HKCR \setminus wow6432 node \\ clsid \setminus \{4590f811-1d3a-11d0-891f-00aa004b2e24\}[]
 Oueries value:
                           HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
 Oueries value:
00aa004b2e24}\inprocserver32[1
                          HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
 Queries value:
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]
                           HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
 Queries value:
                           HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Oueries value:
 Oueries value:
                           00c04fb68820}\proxystubclsid32[]
                           HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
 Oueries value:
 Queries value:
                           HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
```

```
00aa004b2e24}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[]
                                       HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:
                                      HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32[]
                                      HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
  Oueries value:
  Oueries value:
                                       HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Oueries value:
00c04fd8fdff}\inprocserver32[]
  Queries 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]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
  Queries value:
                                       HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:
                                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:
                                       HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32[]
                                       HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
  Queries value:
  Queries value:
                                       HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
                                       HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Queries value:
ce99a996d9ea}\inprocserver32[]
                                      HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Oueries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                                      HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
  Oueries value:
                                      HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
  Queries value:
252725d697ca}\inprocserver32[inprocserver32]
  Queries value:
                                      HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[]
                                       HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
  Queries value:
252725d697ca}\inprocserver32[threadingmodel]
                                      HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
  Queries value:
00000000001}\proxystubclsid32[]
                                      HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
  Queries value:
                                      Oueries value:
00104b703efd}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
  Oueries value:
00104b703efd}\inprocserver32[]
                                       HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
  Oueries value:
00104b703efd}\inprocserver32[threadingmodel]
  Queries value:
                                      HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4395-11d2-b60b-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-1c1c45ee-4390-
00104b703efd}\proxystubclsid32[]
                                      HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
  Oueries value:
00104b703efd}\proxystubclsid32[]
                                       HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}[]
  Queries value:
  Oueries value:
                                      HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
  Queries value:
00c04fb68820}\inprocserver32[1
                                      Queries value:
00c04fb68820}\inprocserver32[threadingmodel]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings\connections[savedlegacysettings]
  Value changes:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\content[cacheprefix]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Value changes:
settings\5.0\cache\history[cacheprefix]
  Value changes:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
```

HKCU\software\microsoft\windows\currentversion\internet

Value changes:

settings\zonemap[autodetect]