# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 3327, Task ID: 815

Task ID: 815 Risk Level: 10

Date Processed: 2016-05-18 10:41:35 (UTC)

Processing Time: 17.13 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe"

Sample ID: 3327
Type: basic
Owner: admin

Label: 6f2064e626e4383a5d8a9c0bdb8e9ddf

Date Added: 2016-05-18 10:30:51 (UTC)

File Type: PE32:win32:gui File Size: 118784 bytes

MD5: 6f2064e626e4383a5d8a9c0bdb8e9ddf

SHA256: d0fae395b7a83a222a795282e88c1d87ca83c3499a2a343f607b8e6c5832cd27

Description: None

# Pattern Matching Results

3 HTTP connection - response code 200 (success)

4 Terminates process under Windows subfolder

10 Creates malicious events: Beebone [Trojan]

6 Checks task list from command line

#### Process/Thread Events

Creates process: C:\windows\temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

["C:\windows\temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe"]

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

tasklist&&del 6f2064e626e4383a]

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\6f2064e626e4383a5d8a9c0bdb8e9ddf.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 \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

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

6F2064E626E4383A5D8A9C0BDB8E9DDF.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

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\U40WOGSM.txt

Opens: C:\Windows\Prefetch\6F2064E626E4383A5D8A9C0BDB8E9-65666C45.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

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

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

Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll

```
C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C:\Windows\SysWOW64\sxs.dll
 Opens:
                         C:\Windows\SysWOW64\winmm.dll
                         C:\Windows\SysWOW64\winmmbase.dll
 Opens:
                         C:\Windows\SysWOW64\lz32.dll
 Opens:
 Opens:
                         C:\
                         C:\Windows\SysWOW64\iertutil.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\Windows\SysWOW64\secur32.dll
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
 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-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
 Opens:
                         C:\Windows\SysWOW64\ws2_32.dll
                         C:\Windows\SysWOW64\winhttp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\Windows\SysWOW64\clbcatq.dll
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc.dll
                         C:\Windows\System32\Drivers\etc\hosts
 Opens:
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.DLL
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\U40WOGSM.txt
                         C:\Windows\SysWOW64\propsys.dll
 Opens:
 Opens:
                         4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db
                         C:\Windows\SysWOW64\desktop.ini
 Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\propsys.dll.mui
 Opens:
                         C:\Users\Admin\Desktop\desktop.ini
 Opens:
                         C:\Windows\SysWOW64\cfgmgr32.dll
 Opens:
                         C:\Windows\SysWOW64\devobj.dll
 Opens:
                         C:\Windows\SysWOW64\setupapi.dll
                         C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cmd.exe
 Opens:
                         C:\Windows\WINHELP.INI
                         C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
 Opens:
 Opens:
 Opens:
                         C:\Windows\Globalization
                         C:\Windows\Globalization\Sorting
 Opens:
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\SysWOW64\wbem
                         C:\Windows\System32\ntdll.dll
 Opens:
 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\System32\conhost.exe
 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
 Opens:
                         C:\Windows\System32\en-US\user32.dll.mui
 Opens:
                         C:\Windows\system32\uxtheme.dll.Config
                         C:\Windows\WinSxS\amd64_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
                         C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
 Opens:
                         C:\Windows\System32\SHCore.dll
 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 C:\Windows\SysWOW64\netapi32.dll Opens: Opens: C:\Windows\SysWOW64\dbghelp.dll Opens: C:\Windows\SysWOW64\netutils.dll Opens: C:\Windows\SysWOW64\srvcli.dll C:\Windows\SysWOW64\wkscli.dll Opens:

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

Opens: C:\Windows\SysWOW64\wbemcomn.dll Opens: C:\Windows\SysWOW64\winsta.dll Opens: C:\Windows\SysWOW64\wbem\wbemsvc.dll C:\Windows\SysWOW64\wbem\fastprox.dll Opens: Opens: C:\Windows\SysWOW64\wbem\wmiutils.dll C:\Windows\SysWOW64\wbem\en-US\wmiutils.dll.mui Opens:

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

Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\U40WOGSM.txt

Reads from: C:\Windows\Temp\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

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: domai.noip1.org

DNS response: domai.noip1.org ⇒ 69.195.129.70

69.195.129.70:443 Connects to: Sends data to: 0.0.0.0:53

Sends data to: domai.noip1.org:443 (69.195.129.70)

Receives data from: 0.0.0.0:53

Receives data from: domai.noip1.org:443 (69.195.129.70)

### 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\

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

settings\p3p\history

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

Creates key: HKCU\software

Creates key: HKCU\software\microsoft

Creates key: HKCU\software\microsoft\visual basic

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

HKCU\software\microsoft\windows\currentversion\internet Deletes value: settings[proxyserver]

Deletes value:

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

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

settings[autoconfigurl]

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

settings[autodetect]

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

settings\zonemap[proxybypass]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[intranetname]

HKLM\software\microsoft\wow64 Opens key:

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

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

 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ safer\+ code identifiers$ Opens key: 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 HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key:

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

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

HKCU\ 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\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

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:

 $\label{thm:linear} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabula$ 

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:  ${\tt HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows}$ 

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

Opens key: HKLM\system\currentcontrolset\control\nls\codepage
Opens key: HKLM\software\wow6432node\microsoft\vba\monitors
Opens key: HKLM\system\currentcontrolset\services\disk\enum

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

Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

Opens key:  ${\tt HKLM \setminus software \setminus wow6432 node \setminus policies \setminus microsoft \setminus windows\ nt \setminus rpc}$ 

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

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

settings\5.0\cache

Opens key:

 $HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| \verb|\windows| current version \verb|\explorer| folder descriptions | the folder description | the fol$ 

Opens key

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

Opens key:

 $\label{thm:local-base-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{352481e8-33be-4251-ba85-6007} caed \cf9d \property bag$ 

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

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ constant \ for the property of the$ 

Opens key:

 $\label{thm:linear} HKCU \software \microsoft \windows \current version \explorer \session in folders \cite{thm:linear} and \cite{t$ 

Opens key: HKU\

Opens key: HKU\.default

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user

 ${\it shell folders}$ 

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

nt\currentversion\profilelist

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

folders Opens kev:

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

settings Opens key:

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

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

settings

```
HKLM\software\wow6432node\policies\microsoft\internet
 Opens key:
explorer\main\featurecontrol
 Opens key:
                         \label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main \+ feature control
                         HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
                         \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ internet explorer \verb+ main \verb+ feature control \\
 Opens kev:
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_http_username_password_disable
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature http username password disable
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                         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
 Opens key:
                         HKCU\software\microsoft\internet
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
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKCU\software\microsoft\internet
 Opens key:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKCU\software\microsoft\internet
 Opens key:
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
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature exclude invalid client cert kb929477
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature return failed connect content kb942615
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                         HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\feature\_preserve\_spaces\_in\_filenames\_kb952730

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

Opens key: HKLM\software\wow6432node

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

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

settings

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

settings\5.0\cache

Opens key:

HKLM\software\wow6432node\nolicies\microsoft\windows\currentyersion\internet settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266 HKCU\software\microsoft\internet

Opens key: explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543

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

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\2d4511fd

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9

Opens key:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ 00000005$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries

Opens key: 

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007 Opens kev:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000000 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 key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

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

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

migration\providers\tcpip6

Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient

Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

Opens key: HKLM\system\currentcontrolset\services\dns

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

nt\dnsclient\dnspolicyconfig

Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig

Opens key:

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:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 152785-66ba-4fcf-9d55-7b8e7f157091 \property bag$ 

Opens key:

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

Opens key:

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

 $Opens~key: \\ HKLM \software \wow 6432 node \microsoft \windows \\ nt \current version \profile list \s-1-5-21-1923240461-1905901954-2556564120-1001 \\ \label{eq:linear_profile}$ 

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:

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

Opens key

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescrip$ 

Opens key:

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

Opens key:

 $\label{lem:hklmsoftwarewow6432} Hklm\soft\ware\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$ 

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

settings\5.0\cache\history

Opens key:

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

Opens key:

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

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

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

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

Opens key: HKLM\software\microsoft\windowsruntime\clsid

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

000000000046}

Opens key: HKCR\activatableclasses\clsid

000000000046}

 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-c000-00000000046} Opens key: HKCU\software\classes\activatableclasses\clsid

000000000046}

Opens key: HKCU\software\classes\appid\6f2064e626e4383a5d8a9c0bdb8e9ddf.exe

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

Opens key:

```
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
    Opens key:
                                                        HKLM\software\policies\microsoft\cryptography
                                                        HKLM\software\microsoft\cryptography
    Opens key:
    Opens key:
                                                        HKLM\software\wow6432node\microsoft\cryptography\offload
    Opens key:
                                                        000000000046}
                                                        HKCR\wow6432node\interface\{00000134-0000-0000-c000-00000000046}
    Opens key:
    Opens key:
                                                        00000000046}\proxystubclsid32
                                                        HKCR\wow6432node\interface\{00000134-0000-0000-c000-
    Opens kev:
000000000046 \} \verb|\proxystubclsid32|
   Opens key:
                                                        HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{a168 \\ add \\ c-1674-49 \\ da-ad4f-1674-49 
4f27df8760d0}
    Opens key:
                                                        HKCR \setminus \{a168aadc-1674-49da-ad4f-4f27df8760d0\}
    Opens key:
                                                        HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32
    Opens key:
                                                        HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32
                                                        HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-
   Opens key:
60ce2149e33c}
    Opens key:
                                                        HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
                                                        Opens kev:
60ce2149e33c}
    Opens key:
                                                        HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
                                                        Opens key:
60ce2149e33c}\treatas
    Opens key:
                                                        HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas
                                                        HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
    Opens key:
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
                                                        HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
   Opens kev:
60ce2149e33c}\inprochandler
                                                        HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
    Opens key:
60ce2149e33c}\inprochandler
    Opens key:
Opens kev:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                                        HKLM\software\wow6432node\microsoft\internet
    Opens kev:
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
    Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus micro
settings\zonemap\domains\
    Opens key:
                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zonemap\domains\
                                                        HKLM\zonemap\ranges\
    Opens key:
                                                        HKCU\zonemap\ranges\
    Opens kev:
    Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                                        HKLM\software\wow6432node\microsoft\internet
    Opens key:
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:hklmsoftware policies microsoft windows \current version \ \ internet
settings\zonemap
   Opens kev:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
    Opens key:
                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
    Opens key:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
                                                        HKCU\software\microsoft\windows\currentversion\internet
    Opens kev:
settings\zonemap\ranges\
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
   Opens kev:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
    Opens key:
                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
    Opens key:
                                                        HKLM\software\policies\microsoft\internet explorer\security
```

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 PKCU\software\microsoft\windows\currentversion\internet settings\zones\0 PKCU\software\microsoft\windows\currentversion\internet settings\zones\1 PKCU\software\microsoft\windows\currentversion\internet settings\zones\1

```
Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 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\currentversion/internet
settings\zones
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
 Opens key:
                          \label{lem:hklm} \verb+Kklm \+ olicies + microsoft + windows + current version + internet
settings\zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet_settings\zones\1
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\1
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
                           HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
                          HKLM\software\wow6432node\microsoft\internet
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 kev:
settings\lockdown_zones
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
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 \verb|\policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\1
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ 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:
settings\lockdown_zones\2
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\lockdown_zones\2
 Opens key:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                          HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
```

```
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
     Opens key:
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
    Opens key:
                                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                                        HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\lockdown_zones\4
     Opens key:
settings\lockdown_zones\4
    Opens key:
                                                                        HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
     Opens key:
                                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
                                                                        HKCU\software\microsoft\internet
    Opens kev:
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                                                        HKLM\software\wow6432node\microsoft\internet
    Opens key:
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\winhttp
                                                                        HKLM\system\currentcontrolset\services\winhttpautoproxysyc\parameters
     Opens kev:
     Opens key:
                                                                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                                                                        HKLM\software\wow6432node\policies\microsoft\system\dnsclient
     Opens key:
     Opens key:
                                                                         HKLM\software\policies\microsoft\system\dnsclient
     Opens key:
HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40544401-87b7-40544401-87b7-40544401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-875
 55779daa70e9}
    Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
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:
25b8d56dd1d8}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
     Opens key:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8
55779daa70e9}
     Opens key:
                                                                         {\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| linkage \\
     Opens key:
                                                                         \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\p3p\history\noip1.org
     Opens key:
                                                                        HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
 types\type 001
     Opens kev:
Opens key:
                                                                         HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ 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:
HKLM \label{lem:hklm} Which is the latest and the
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{031e4825-
7b94-4dc3-b131-e946b44c8dd5}
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{04731b67-1000}
d933-450a-90e6-4acd2e9408fe}
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-
e366-4d22-bc06-4ada335c892b}
HKLM\software\www6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{26ee0668-
a00a-44d7-9371-beb064c98683}
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{4336a54d-
038b-4685-ab02-99bb52d3fb8b}
ad25-11d0-98a8-0800361b1103}
     Opens key:
```

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

Opens key: HKLM\software\www6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{59031a47-3f72-44a7-89c5-5595fe6b30ee} Opens key: 5081-101b-9f08-00aa002f954e} Opens key: 1c21-4f30-a98f-4e52906d3b56} Opens key: 6bd1-4c86-9454-beb04e94c819} Opens key: 1c37-4a49-a12e-4b2d810d956b} Opens key: 4fff-11e0-89e2-7b86dfd72085} Opens key:  $HKLM \label{lem:hklm} Which is the label of the label o$ ebd9-48b8-944a-8942113d46ac} Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{b4fb3f98-b4fb3f98$ c1ea-428d-a78a-d1f5659cba93} Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ name space \ \{bd7a2e7b-parent \ bd7a2e7b-parent \ bd7a2e7b-$ 21cb-41b2-a086-b309680c6b7e} Opens key: e44d-46af-be1b-cbacea2c3065} Opens kev: 9397-435c-8f95-4e922c26259e} Opens key: 9ea8-4870-83b1-96b02cfe0d52} Opens kev: 4d53-4b2f-a265-5805674be568} Opens key: be21-4350-88b0-7367fc96ef3c} Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders Opens key: Opens kev:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session info \ 1 \ desktop \ manespace \ delegate folders$ HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens kev: 08002b30309d}\shellfolder HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key: 08002b30309d}\shellfolder  $HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + (20d04feo-block) +$ Opens key: 3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: a2d8-08002b30309d}\shellfolder HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKCU\software\classes\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-Opens kev: 08002b30309d}\shellfolder HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-Opens kev: 08002b30309d}\shellfolder  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{208d2c60-microsoft \setminus windows \setminus current version \setminus clsid \setminus explorer \setminus clsid$ Opens key: 3aea-1069-a2d7-08002b30309d}\shellfolder Opens kev: a2d7-08002b30309d}\shellfolder HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-Opens kev: 08002b30309d}\shellfolder Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder Opens key: 42a0-1069-a2ea-08002b30309d}\shellfolder

HKCU\software\classes\wow6432node\clsid\{645ff040-5081-101b-9f08-Opens kev: 00aa002f954e}\shellfolder Opens key: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \end{tabular} $$ (645ff 040-100) $$ (45ff 040-1000) $$ (45ff 040-100) $$ (45ff 040-1000) $$ (45ff 040-$ 

```
5081-101b-9f08-00aa002f954e}\shellfolder
             Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (645 ff 040 - 5081 - 101 b-101 b
 9f08-00aa002f954e}\shellfolder
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
             Opens kev:
 beb064c98683}\shellfolder
             Opens key:
                                                                                                                                                                                           HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
  beb064c98683}\shellfolder
                                                                                                                                                                                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \clsid \class{lem:hkcu} \end{tabular} $$ 1.00 \mbox{ and } 1.00 \mbox{ an
             Opens key:
 a00a-44d7-9371-beb064c98683}\shellfolder
            Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{26ee 0668-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-a00a-44d7-
  9371-beb064c98683}\shellfolder
            Opens kev:
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 5595fe6b30ee}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 5595fe6b30ee}\shellfolder
                                                                                                                                                                                            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
             Opens key:
 3f72-44a7-89c5-5595fe6b30ee}\shellfolder
             Opens key:
 89c5-5595fe6b30ee}\shellfolder
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
             Opens kev:
  e946b44c8dd5}\shellfolder
                                                                                                                                                                                           HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
            Opens key:
  e946b44c8dd5}\shellfolder
                                                                                                                                                                                            HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{031e4825-explorer\} \setminus \{031e4825
             Opens key:
  7b94-4dc3-b131-e946b44c8dd5}\shellfolder
             Opens kev:
 b131-e946b44c8dd5}\shellfolder
                                                                                                                                                                                           HKCU\software\classes\wow6432node\clsid\{04731b67-d933-450a-90e6-
             Opens key:
  4acd2e9408fe}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 4acd2e9408fe}\shellfolder
                                                                                                                                                                                            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{04731b67-
             Opens key:
 d933-450a-90e6-4acd2e9408fe}\shellfolder
             Opens key:
 HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{04731b67-d933-450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d933-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d9340a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93450a-d93400a-d93450a-d93450a-d9340a-d93450a-d93450a-d93450a-d93450a-d93450
 90e6-4acd2e9408fe}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{11016101-e366-4d22-bc06-
  4ada335c892b}\shellfolder
                                                                                                                                                                                           HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
            Opens kev:
 4ada335c892b}\shellfolder
                                                                                                                                                                                            HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{11016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-1016101-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-101610-1016100-101610-101610-101610-101610-101610-101610-101610-101610-10161
             Opens kev:
 e366-4d22-bc06-4ada335c892b}\shellfolder
             Opens key:
 bc06-4ada335c892b}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{4336a54d-038b-4685-ab02-
  99bb52d3fb8b}\shellfolder
                                                                                                                                                                                           HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
            Opens kev:
  99bb52d3fb8b}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{4336a54d-microsoft \setminus windows \setminus current version \setminus clsid \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus
 038b-4685-ab02-99bb52d3fb8b}\shellfolder
             Opens key:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{4336a54d-038b-4685-
 ab02-99bb52d3fb8b}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
  0800361b1103}\shellfolder
            Opens key:
                                                                                                                                                                                           HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
  0800361b1103}\shellfolder
                                                                                                                                                                                            HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (450d8fba-microsoft) \setminus (450d8fba-microsoft)
             Opens key:
 ad25-11d0-98a8-0800361b1103}\shellfolder
             Opens key:
 HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{450d8fba-ad25-11d0-d848fba-ad25-11d0-d848fba-ad25-11d0-d848fba-ad25-11d0-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848fba-ad25-d848f
 98a8-0800361b1103}\shellfolder
            Opens key:
                                                                                                                                                                                            HKCU\software\classes\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
  1d8870fdcba0}\shellfolder
                                                                                                                                                                                           HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
             Opens kev:
  1d8870fdcba0}\shellfolder
             Opens key:
                                                                                                                                                                                            HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{5399e694-694-694694\} \ description \ for the software \ description \ descri
  6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder
             Opens key:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{5399e694-6ce5-4d6c-
 8fce-1d8870fdcba0}\shellfolder
             Opens key:
                                                                                                                                                                                            4e52906d3b56}\shellfolder
                                                                                                                                                                                          HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
            Opens kev:
 4e52906d3b56}\shellfolder
             Opens key:
                                                                                                                                                                                           HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{64693913 - microsoft \setminus windows \setminus current version \setminus clsid \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus clsid \setminus cl
  1c21-4f30-a98f-4e52906d3b56}\shellfolder
             Opens key:
```

```
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (explorer \ clsid) \ \{64693913-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30-1c21-4f30
a98f-4e52906d3b56}\shellfolder
         Opens key:
                                                                                                                                       HKCU\software\classes\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder
                                                                                                                                      HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
         Opens kev:
beb04e94c819}\shellfolder
         Opens key:
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\clsid\{89d83576-
 6bd1-4c86-9454-beb04e94c819}\shellfolder
         Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{89d83576-6bd1-4c86-
9454-beb04e94c819}\shellfolder
                                                                                                                                       HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{9343812e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a49-a12e-1c37-4a6-1c37-4a6-1c37-4a6-1c37-4a6-1c37-4a6-1c37-4a6-1c37-4a6-1c37-4a6-1c3
         Opens key:
4b2d810d956b}\shellfolder
                                                                                                                                      HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
        Opens key:
4b2d810d956b}\shellfolder
                                                                                                                                       HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9343812e-
         Opens key:
 1c37-4a49-a12e-4b2d810d956b}\shellfolder
         Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{9343812e-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a49-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7-1c37-4a7
a12e-4b2d810d956b}\shellfolder
                                                                                                                                       Opens key:
 7b86dfd72085}\shellfolder
                                                                                                                                      HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
         Opens kev:
 7b86dfd72085}\shellfolder
                                                                                                                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{98f275b4-terminal explorer \setminus clsid \setminus
        Opens key:
4fff-11e0-89e2-7b86dfd72085}\shellfolder
         Opens key:
89e2-7b86dfd72085}\shellfolder
                                                                                                                                       HKCU\software\classes\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
         Opens key:
 8942113d46ac}\shellfolder
                                                                                                                                      HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
         Opens key:
 8942113d46ac}\shellfolder
                                                                                                                                       HKCU\software\microsoft\windows\currentversion\explorer\clsid\{a00ee528-
         Opens key:
 ebd9-48b8-944a-8942113d46ac}\shellfolder
944a-8942113d46ac}\shellfolder
                                                                                                                                       HKCU\software\classes\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
         Opens key:
d1f5659cba93}\shellfolder
         Opens key:
                                                                                                                                      HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\clsid\{b4fb3f98-
        Opens kev:
 c1ea-428d-a78a-d1f5659cba93}\shellfolder
         Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ clsid \ \{b4fb3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-c1ea-428d-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1464b3f98-f1
a78a-d1f5659cba93}\shellfolder
         Opens key:
                                                                                                                                       b309680c6b7e}\shellfolder
         Opens key:
                                                                                                                                      HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
 b309680c6b7e}\shellfolder
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\clsid\{bd7a2e7b-
         Opens kev:
21cb-41b2-a086-b309680c6b7e}\shellfolder
         Opens key:
a086-b309680c6b7e}\shellfolder
         Opens kev:
                                                                                                                                       HKCU\software\classes\wow6432node\clsid\{daf95313-e44d-46af-be1b-
 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 clsid \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-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-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-daf9
        Opens key:
 e44d-46af-be1b-cbacea2c3065}\shellfolder
         Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus (daf 95313 - e44d - 46af - e44d - e46af 
be1b-cbacea2c3065}\shellfolder
                                                                                                                                       HKCU\software\classes\wow6432node\clsid\{e345f35f-9397-435c-8f95-
         Opens kev:
4e922c26259e}\shellfolder
                                                                                                                                      HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
        Opens key:
 4e922c26259e}\shellfolder
                                                                                                                                      HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{e345f35f-icrosoft \setminus windows \setminus explorer \setminus clsid \setminus \{e345f35f-icrosoft \setminus explorer \setminus explo
        Opens kev:
9397-435c-8f95-4e922c26259e}\shellfolder
         Opens kev:
HKLM\software\www6432node\microsoft\windows\currentyersion\explorer\clsid\{e345f35f-9397-435c-
8f95-4e922c26259e}\shellfolder
         Opens key:
                                                                                                                                       96b02cfe0d52}\shellfolder
         Opens key:
                                                                                                                                       96b02cfe0d52}\shellfolder
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\clsid\{ed228fdf-
        Opens key:
 9ea8-4870-83b1-96b02cfe0d52}\shellfolder
         Opens key:
83b1-96b02cfe0d52}\shellfolder
```

Opens key: HKCU\software\classes\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-

5805674be568}\shellfolder

Opens key: HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-

5805674be568}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{edc978d6-

4d53-4b2f-a265-5805674be568}\shellfolder

Opens kev:

a265-5805674be568}\shellfolder

Opens key: HKCU\software\classes\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-

7367fc96ef3c}\shellfolder

Opens key: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-

7367fc96ef3c}\shellfolder

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

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

Opens key:

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

88b0-7367fc96ef3c}\shellfolder

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

paths\cmd.exe

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

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

08002b30309d}\inprocserver32

Opens key:

 $\label{thm:linear} \mbox{HKCU\software\mbox{\sc windows\currentversion\explorer\mbox{\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\sc windows\currentversion\explorer\explor$ 

Opens key:

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

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

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens key: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

 $\begin{tabular}{ll} Opens~key: & HKCR\allfilesystemobjects\browseinplace \\ Opens~key: & HKCU\software\classes\directory\clsid \\ \end{tabular}$ 

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\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

Opens key:  $\label{eq:hkkcr} \begin{tabular}{ll} HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}} \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}. \\ \end{tabular}$ 

b8dc300d9f9d}

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

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}

b8dc300d9f9d}\treatas

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

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: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKCU\software\classes\.exe\openwithprogids

Opens key: HKCR\.exe\openwithprogids

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\openwithprogids

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

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

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

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

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

Opens key: HKCR\exefile\docobject

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

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

Opens key: HKCR\exefile\browseinplace

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

Opens key: HKCR\systemfileassociations\.exe\browseinplace

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:

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

Opens key:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\folderdescriptions\gamma\folderdescriptions\gamma\gamma\folderdescriptions\gamma\g$ 

Opens key:

Opens kev:

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} b3ea5dc-b587-4786-b4ef-bd1dc332 aeae} \property bag$ 

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

Opens key: HKCR\exefile\shell

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

Opens key: HKCR\exefile\shell\open

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

5c9f68572fd1}\inprocserver32

Opens key: HKCR\exefile\shell\open\

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

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

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

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{76765b11-3f95-4af2-ac9d-

ea55d8994f1a}

 $\label{lem:continuous} Opens~key: & HKCR\activatableclasses\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a} \\ Opens~key: & HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a} \\ \\ Opens~key: & HKCU\software\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\classes\wow6432node\clsid\clsid\classes\wow6432node\clsid\$ 

ea55d8994f1a}

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

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

ea55d8994f1a}\treatas

ea55d8994f1a}\inprocserver32

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

ea55d8994f1a}\inprocserver32

 $Opens~key: \\ HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{76765b11-3f95-4af2-ac9d-14812$ 

ea55d8994f1a}\inprochandler32

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

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

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

ea55d8994f1a}\inprochandler32

Opens key:

11e3-be65-806e6f6e6963}\

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

ea55d8994f1a}\inprochandler

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

ea55d8994f1a}\inprochandler

 $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{7b8a2d94 - 0ac9 - 11d1 - 896c - 12d1 - 12$ Opens key:

00c04fb6bfc4}

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

00c04fb6bfc4}

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

00c04fb6bfc4}\treatas

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

00c04fb6bfc4}\inprocserver32

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

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

HKCU\software\microsoft\internet Opens key:

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

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_zones\_default\_drive\_intranet\_kb941000 Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ internet$ explorer\main\featurecontrol\feature\_zones\_default\_drive\_intranet\_kb941000

HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_protocol\_lockdown

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

explorer\main\featurecontrol\feature\_protocol\_lockdown

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

settings\zones\0

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

Opens key:

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

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

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

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

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

Opens key:

Opens key:

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

Opens key:

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

Opens kev:

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

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

Opens key:

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

HKCU\software\classes\exefile\shell\open\ddeexec Opens kev:

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

Opens key: HKLM\software\policies\microsoft\windows\appcompat Opens key: HKCU\software\microsoft\windows nt\currentversion

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

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

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:  $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constant of the constan$ Opens key:

Opens kev: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

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

Opens key: HKCR\applications\cmd.exe

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

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

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

options\conhost.exe

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

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

Opens key: HKLM\software\microsoft\oleaut

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

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

Opens key: HKCU\console\%systemroot%\_system32\_cmd.exe HKCU\console\%systemroot%\system32\cmd.exe Opens key:

Opens key: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange Opens key: HKLM\software\microsoft\ctf\compatibility\conhost.exe HKLM\software\microsoft\windows\windows error reporting\wmr Opens kev:

Opens key:

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

Opens key: HKCU\software\microsoft\command processor

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

options\tasklist.exe

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

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:  $HKLM \ software \ wow 6432 node \ microsoft \ wbem \ cimom$ 

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}

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

Opens key:

HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas  $HKCR \setminus wow 6432 node \\ clsid \\ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \\ \setminus treat as$ 

Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32

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

00aa004b2e24}\inprocserver32

Opens key: 00aa004b2e24}\inprochandler32

Opens key:

HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32

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

00aa004b2e24}\inprochandler

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

00aa004b2e24}\inprochandler

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

Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{8bc3f05e-d86b-11d0-a075-d86b-11d0-a07$ 

00c04fb68820}

Opens key:

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

HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key:

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8bc3f05e-d86b-11d0-a075-$ 00c04fb68820}\treatas

Opens kev:

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

00c04fb68820}\inprocserver32

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

00c04fb68820}\inprocserver32

Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8bc3f05e-d86b-11d0-a075-$ 

00c04fb68820}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a07500c04fb68820}\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:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{f309 \\ ad 18 - d86 \\ a-11 \\ d0-a075 - d86 \\ a-11 \\ a-1$ 00c04fb688201  $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{f309 \\ ad18 - d86 \\ a-11 \\ d0-a075-00 \\ c04 \\ fb68820\}$ Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32 HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-Opens kev: 00c04fb68820}\proxystubclsid32 Opens key: HKLM\software\microsoft\windowsruntime\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key:  $HKCR \land ctivatable classes \land clsid \land \{7c857801-7381-11cf-884d-00aa004b2e24\}$ Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{7c857801 - 7381 - 11cf - 884d - 11cf - 884d$ 00aa004b2e24}\treatas Opens key:  $HKCR \ wow 6432 node \ clsid \ \{7c857801-7381-11cf-884d-00aa 004b2e24\} \ treat as the control of the control$ Opens key:  $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-8$ 00aa004b2e24}\inprocserver32 HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler32 HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-Opens kev: 930efe48a887}\proxystubclsid32 HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-Opens key: 930efe48a887}\proxystubclsid32 Opens key HKLM\software\microsoft\windowsruntime\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} 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 Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev 00c04fd8fdff}\inprochandler HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} Opens kev:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{9556 \\ dc99-828 \\ c-11 \\ cf-a37 \\ e-11 \\ cf-a37 \\ e-12 \\ e-1$ Opens key: 00aa003240c7}\proxystubclsid32 HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-Opens key: 00aa003240c7}\proxystubclsid32 Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea} Opens key: HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea} Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{d68af00a-29cb-43fa-8504-468af00a-29cb-436af00a-29$ ce99a996d9ea}\treatas Opens key:  $HKCR\wow6432 node \verb|\clsid|{d68af00a-29cb-43fa-8504-ce99a996d9ea} \verb|\treatas|$ Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

Opens key:  $\label{lem:hcusoftware} HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\$ 

ce99a996d9ea}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprochandler HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\inprochandler Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-252725d697ca3 Opens key: HKCR\activatableclasses\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens key: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens key:  $HKCR \ wow 6432 node \ clsid \ \{e7d35cfa-348b-485e-b524-252725d697ca\}$ Opens key: 252725d697ca}\treatas Opens key:  $HKCR\wow6432 node \clsid \{e7d35cfa-348b-485e-b524-252725d697ca\} \treat as$ Opens key: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprocserver32 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens key: 252725d697ca}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens key: 252725d697ca}\inprochandler32 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens key: 252725d697ca}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens key: 252725d697ca}\inprochandler HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens key: 252725d697ca}\inprochandler Opens key: 000000000013 Opens key: Opens kev: 00000000001}\proxystubclsid32 HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-Opens key: 00000000001}\proxystubclsid32

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

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

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

00104b703efd}

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

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

00104b703efd}\treatas

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

00104b703efd}\inprocserv er32

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

00104b703efd}\inprocserver32

Opens key: 

00104b703efd}\inprochandler32

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

00104b703efd}\inprochandler32

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

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}

HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd} Opens kev:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{1c1c45ee-4395-11d2-b60b-432 \\ node \setminus interface \setminus \{1c1c45ee-430b-432 \\ node \setminus \{1c1c45ee-430b-4$ Opens key: 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} HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-Opens key:

00104b703efd}\proxystubclsid32

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

00104b703efd}\proxystubclsid32

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

00c04fb68820}

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

Opens key:  $HKCR \ wow 6432 node \ clsid \ \{eb87e1bd-3233-11d2-aec9-00c04fb68820\}$ Opens kev: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-

00c04fb68820}\treatas

Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas 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:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{eb87e1bd-3233-11d2-aec9-ber0432 \\ node \setminus clsid \setminus \{eb87e1bd-3233-11d2-aec9-ber042 \\ node \setminus clsid \setminus \{eb87e1bd-3233-11d2-aec9-ber042 \\ node \setminus$  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\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrol\terminal server[tsuserenabled]

Queries value:

Oueries value:

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

Queries value: HKLM\system\currentcontrolset\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:

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.dll]

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

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[6f2064e626e4383a5d8a9c0bdb8e9ddf]
Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

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

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

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

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

manager[safeprocesssearchmode]

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

 Queries value:
 HKLM\system\currentcontrol\set\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\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\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

```
33be-4251-ba85-6007caedcf9d}[relativepath]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[parsingname]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[infotip]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[localizedname]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[icon]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[security]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresource]
  Queries value:
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[localredirectonly]
  Queries value:
33be-4251-ba85-6007caedcf9d}[roamable]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[precreate]
  Queries value:
33be-4251-ba85-6007caedcf9d}[stream]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
  Queries value:
33be-4251-ba85-6007caedcf9d}[attributes]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[foldertypeid]
  Queries value:
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
  Queries value:
                                       HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| user | leads to be a considered for the constraints of the constraints
shell folders[cache]
                                        HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
  Oueries value:
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Oueries value:
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
  Queries value:
                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]
                                       HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature http username password disable[*]
                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                       HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_mime_handling[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]
                                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature mime handling[*]
  Queries value:
                                       explorer \verb|\main| featurecontrol| feature_disable_unicode_handle_closing_callback[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]|
  Oueries value:
                                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Oueries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:
                                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                        \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu
  Oueries value:
settings[secureprotocols]
  Queries value:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
```

settings[disablekeepalive]

```
Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
   Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[preconnectlimit]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[preresolvelimit]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[sqmhttpstreamrandomuploadpoolsize]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablehttp1_1]
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[enablehttp1_1]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[proxyhttp1.1]
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyhttp1.1]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[proxyhttp1.1]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablenegotiate]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablebasicoverclearchannel]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[clientauthbuiltinui]
                                                  \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings[enableautoproxyresultcache]
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[displayscriptdownloadfailureui]
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[mbcsservername]
                                                  \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings[utf8servernameres]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disableworkerthreadhibernation]
                                                  HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
   Queries value:
settings[disableworkerthreadhibernation]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketsendbufferlength]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[socketreceivebufferlength]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[maxhttpredirects]
   Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
   Queries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[maxconnectionsper1_0server]
   Oueries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
   Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[serverinfotimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[connecttimeout]
   Queries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[connectretries]
   Queries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
   Queries value:
                                                  HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[receivetimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablentlmpreauth]
   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} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[scavengecachelowerbound]
   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} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
```

```
settings[certcachenovalidate]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  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[ftpdefaultexpirytimesecs]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[leashlegacycookies]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                                    \label{thm:local_microsoft} \begin{tabular}{ll} HKLM \end{tabular} software \begin{tabular}{ll} wow 6432 node \end{tabular} microsoft \begin{tabular}{ll} windows \end{tabular} current version \end{tabular} in terms to the constant of th
  Oueries value:
settings[dialupuselansettings]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendextracrlf]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                                     Queries value:
settings[nocheckautodialoverride]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[mimeexclusionlistforcache]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscacheentries]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnalwaysonpost]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonzonecrossing]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpostredirect]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[alwaysdrainonredirect]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[tcpautotuning]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\0000000000002[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006[packedcatalogitem]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[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\000000000009[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Queries 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]
- $\label{librarypath} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath]\\ Queries\ value: \begin{tabular}{ll} Queries\ value: \end{tabular}$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ solves \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
  Queries 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\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo] Oueries 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\0000000000002[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
  Queries 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] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[enabled]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[displaystring]
  Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog \shape \current \shape \s$

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000004 [supported name space]]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 000000000000004 [enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000004[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]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000005[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005[supported name space]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus ser
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 \ [displaystring]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 000000000006 \ [address family]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 [supported name space]]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000006[enabled]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 10000000000006 \ [storesservice classinfo]
   Queries value:
Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets]
  Queries value:
                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[badproxyexpirestime]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
   Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[globaluseroffline]
                                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
   Queries value:
settings[disablebranchcache]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[combinefalsestartdata]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
   Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[enforcep3pvalidity]
                                          HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\peerdist\service[enable]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyserver]
  Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
                                           HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
```

settings[autodetect]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings] HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: 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] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance] HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [domain named evolution level]$ Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen badtlds]$ Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[screendefaultservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [filter clusterip]$ Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns]  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query net bt fqdn]$ Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value:

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

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]$ HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\svstem\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration] HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping] HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b$ 6fba-4fcf-9d55-7b8e7f157091}[category] Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[name]

Oueries value:

Queries value:

 $HKLM \label{lem:hklm} Which was the statement of the second of the sec$ 6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Queries value:

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

Oueries value:

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[streamresource]$$ 

Oueries value

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

Oueries value:

 $\label{thm:local-reduced} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fib 32785-66 ba-4fcf-9d55-7b8e7f157091 \fill \f$ 

Oueries value:

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

Oueries value

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

Oueries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-65ba-4fcf-9d55-7b8e7f157091\fifth{1}{5}ream\figure{1}{5}$ 

Oueries value

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$157091 $$[foldertypeid] $$$ 

Queries value:

 $\label{thm:local-continuous} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-2785-66ba-4fcf-9d55-7b8e7f157091 \[initfolder \handler]$ 

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

folders[local appdata]

Queries value:

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

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{ali$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Oueries value:

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

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

Oueries value:

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

Queries value:

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

Queries value:

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

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

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

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

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

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]

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

settings\5.0\cache\content[cachelimit]

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16464, 2b0f765d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0$ c0e9-4171-908e-08a611b84ff6}[name]

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16464, 2b0f765d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b$ c0e9-4171-908e-08a611b84ff6}[description]

Queries value:

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

Oueries value:

c0e9-4171-908e-08a611b84ff6}[parsingname] Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[security]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16464, 2b0f765d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b$ c0e9-4171-908e-08a611b84ff6}[streamresource]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value: HKCU\software\microsof

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

folders[cookies]

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [stream]$ 

Queries value:

Oueries value:

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

Queries value:

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

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\[initfolderhandler]

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

folders[appdata]
Oueries value:

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

settings\5.0\cache\cookies[cachelimit]

Oueries value:

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

Queries value:

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

Queries value:

```
b784-432e-a781-5a1130a75963}[parentfolder]
Oueries value:
b784-432e-a781-5a1130a75963}[description]
Queries value:
b784-432e-a781-5a1130a75963}[relativepath]
Oueries value:
b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
b784-432e-a781-5a1130a75963}[infotip]
Queries value:
b784-432e-a781-5a1130a75963}[localizedname]
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d9dc8a3b-delta \} \\ description \setminus \{d9dc8ab-delta \} \\ descript$ 

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d9dc8a3b-delta \} \\ description \setminus \{d9dc8ab-delta \} \\ descript$ 

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d$ 

HKCU\software\microsoft\windows\currentversion\internet

HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]

HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

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

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

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

HKLM\software\microsoft\rpc\extensions[ndroleextdll]

HKLM\software\microsoft\ole[defaultaccesspermission]

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic

HKLM\software\microsoft\cryptography[machineguid]

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

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

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

HKCR\wow6432node\interface\{00000134-0000-0000-c000-

HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-

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

HKLM\software\microsoft\com3[com+enabled]

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

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

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

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

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

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

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

settings\5.0\cache\history[cachelimit]

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

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

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

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

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

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

Queries value:

Oueries value:

Queries value:

folders[history]
Queries value:

Queries value: Queries value:

Queries value: Queries value:

Oueries value:

Queries value:

provider[type]
Oueries value:

Oueries value:

Oueries value:

Queries value: Queries value:

Oueries value:

Oueries value:

Oueries value:

Queries value:

Queries value:

provider[image path]
 Queries value:

000000000046}\proxystubclsid32[]

4f27df8760d0}\proxystubclsid32[]

60ce2149e33c}\inprocserver32[]

60ce2149e33c}\inprocserver32[inprocserver32]

60ce2149e33c}\inprocserver32[threadingmodel] HKLM\software\microsoft\ole[maxsxshashcount] Oueries value: Oueries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata] Oueries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags] HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature\_localmachine\_lockdown[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_localmachine\_lockdown[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] HKCU\software\policies\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[createuricachesize] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[createuricachesize] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] Oueries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autoproxydetecttype] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\winhttp[disablebranchcache] Oueries value: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[winhttplowercasehost] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[1a10] Oueries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp] Queries value: 55779daa70e9}[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain]

Queries value:

```
HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40544401-87b7-40544401-87b7-40544401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-875
55779daa70e9}[nameserver]
    Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus interfaces \setminus \{b5105d63-74c6-4dc1-87b7-47b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1-147b1
55779daa70e9}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
    Oueries value:
806e6f6e6963}[registrationenabled]
    Queries 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]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
    Queries value:
                                                                HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[queryadaptername]
    Queries value:
55779daa70e9}[disableadapterdomainname]
    Queries value:
55779daa70e9}[registrationmaxaddresscount]
    Oueries value:
55779daa70e9}[maxnumberofaddressestoregister]
    Queries value:
55779daa70e9}[enablemulticast]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[queryadaptername]
    Queries value:
```

806e6f6e6963}[disableadapterdomainname]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

806e6f6e6963}[enablemulticast]

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

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

settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]

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

settings[privacyadvanced]

Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider

types\type 001[name]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] Oueries value:

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

Queries value:

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

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

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

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

Oueries value:

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

Oueries 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]

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{11016101-101610-101$ e366-4d22-bc06-4ada335c892b}[suppressionpolicy]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

6ce5-4d6c-8fce-1d8870fdcba0}[suppressionpolicy]

Queries value:

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

Oueries value:

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

Queries value:

1c21-4f30-a98f-4e52906d3b56}[suppressionpolicy]

Oueries value:

6bd1-4c86-9454-beb04e94c819}[suppressionpolicy]

Oueries value:

1c37-4a49-a12e-4b2d810d956b}[suppressionpolicy]

Oueries value:

4fff-11e0-89e2-7b86dfd72085}[suppressionpolicy]

Queries value:

ebd9-48b8-944a-8942113d46ac}[suppressionpolicy]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ desktop \ names pace \ \ \{b4fb3f98-fine \ \ b4fb3f98-fine \ \ \ b4fb3f98-fine \ \ \ b4fb3f98-fine \ \ \ b4fb3f98-fine \$ c1ea-428d-a78a-d1f5659cba93}[suppressionpolicy]

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{daf95313-daf9531-daf9$ e44d-46af-be1b-cbacea2c3065}[suppressionpolicy]

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ namespace \ \{ed 228 fdf-desktop \ namespace \ ed 228 fdf-desktop \ n$ 9ea8-4870-83b1-96b02cfe0d52}[suppressionpolicy]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{edc 978d6-1647846 - 164786 - 164786 - 164786 - 164786 - 164786 -$ 4d53-4b2f-a265-5805674be568}[suppressionpolicy]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ desktop \ namespace \ \ \{f02c1a0d-f02c$ be21-4350-88b0-7367fc96ef3c}[suppressionpolicy]

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

08002b30309d}\shellfolder[attributes]

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

08002b30309d}\shellfolder[callforattributes]

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[foldervalueflags]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-

08002b30309d}1

HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-Oueries value:

08002b30309d}\shellfolder[attributes]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-

08002b30309d}\shellfolder[callforattributes]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-

```
08002b30309d}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
 Oueries value:
08002b30309d}\shellfolder[foldervalueflags]
 Queries value:
08002b30309d}1
 Oueries value:
                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
 Queries value:
                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
 Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
 Queries value:
                        HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[foldervalueflags]
                        HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
 Queries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}]
                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
 Queries value:
00aa002f954e}\shellfolder[attributes]
                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
 Queries value:
00aa002f954e}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
 Queries value:
00aa002f954e}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{645ff040-5081-101b-9f08-
00aa002f954e}]
                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
 Oueries value:
beb064c98683}\shellfolder[attributes]
                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
 Queries value:
beb064c98683}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
 Oueries value:
beb064c98683}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
 Oueries value:
beb064c98683}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{26ee0668-a00a-44d7-9371-
beb064c98683}]
                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Queries value:
5595fe6b30ee}\shellfolder[attributes]
 Queries value:
                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Queries value:
5595fe6b30ee}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
 Queries value:
5595fe6b30ee}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-
5595fe6b30ee}1
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[attributes]
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
 Oueries value:
e946b44c8dd5}\shellfolder[callforattributes]
 Oueries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[restrictedattributes]
 Queries value:
                        HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[foldervalueflags]
 Queries value:
e946b44c8dd5}1
 Oueries value:
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[attributes]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Queries value:
4acd2e9408fe}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
 Oueries value:
4acd2e9408fe}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{04731b67-d933-450a-90e6-
4acd2e9408fe}]
 Queries value:
                        HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[attributes]
 Queries value:
                        HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[callforattributes]
                        HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
 Oueries value:
4ada335c892b}\shellfolder[restrictedattributes]
                        HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
 Queries value:
4ada335c892b}\shellfolder[foldervalueflags]
 Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{11016101-e366-4d22-bc06-
4ada335c892b}1
 Queries value:
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
 Oueries value:
99bb52d3fb8b}\shellfolder[callforattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
 Queries value:
99bb52d3fb8b}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{4336a54d-038b-4685-ab02-
99bb52d3fb8b}1
 Oueries value:
                         HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[attributes]
 Queries value:
                         HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
 Queries 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}]
                         HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
 Queries value:
1d8870fdcba0}\shellfolder[attributes]
                          HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
 Queries value:
1d8870fdcba0}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
 Oueries value:
1d8870fdcba0}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
 Oueries value:
1d8870fdcba0}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}]
                         HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
 Queries 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]
 Queries value:
                         HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{64693913-1c21-4f30-a98f-
4e52906d3b56}1
 Queries value:
                         HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
 Oueries value:
beb04e94c819}\shellfolder[callforattributes]
 Oueries value:
                         HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[restrictedattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{89d83576-6bd1-4c86-9454-
beb04e94c819}]
                          HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
 Oueries value:
4b2d810d956b}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
 Queries value:
4b2d810d956b}\shellfolder[callforattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
 Oueries value:
4b2d810d956b}\shellfolder[foldervalueflags]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9343812e-1c37-4a49-a12e-
4b2d810d956b}]
 Queries value:
                          HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-646}
7b86dfd72085}\shellfolder[attributes]
 Queries value:
                         HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder[callforattributes]
                         HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
 Oueries value:
7b86dfd72085}\shellfolder[restrictedattributes]
                         HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
 Queries value:
7b86dfd72085}\shellfolder[foldervalueflags]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{98f275b4-4fff-11e0-89e2-
7b86dfd72085}1
 Queries value:
                          HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
 Oueries value:
8942113d46ac}\shellfolder[callforattributes]
```

```
Oueries value:
                                    HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[restrictedattributes]
  Oueries value:
                                    HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[foldervalueflags]
  Oueries value:
8942113d46ac}1
                                    HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
  Oueries value:
d1f5659cba93}\shellfolder[attributes]
  Queries value:
                                    HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[callforattributes]
                                    Queries value:
d1f5659cba93}\shellfolder[restrictedattributes]
  Oueries value:
                                    HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[foldervalueflags]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus monenum [\{b4fb3f98-c1ea-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-428d-a78a-4
d1f5659cba93}]
                                    HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
  Queries value:
b309680c6b7e}\shellfolder[attributes]
                                    HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
  Queries value:
b309680c6b7e}\shellfolder[callforattributes]
                                    Oueries value:
b309680c6b7e}\shellfolder[restrictedattributes]
                                    HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
  Queries value:
b309680c6b7e}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}1
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  Queries value:
cbacea2c3065}\shellfolder[attributes]
  Queries value:
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[callforattributes]
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  Queries value:
cbacea2c3065}\shellfolder[restrictedattributes]
                                    HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
  Queries value:
cbacea2c3065}\shellfolder[foldervalueflags]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{daf95313-e44d-46af-be1b-
cbacea2c3065}1
  Queries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[attributes]
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
  Oueries value:
4e922c26259e}\shellfolder[callforattributes]
  Oueries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[restrictedattributes]
  Queries value:
                                    HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[foldervalueflags]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{e345f35f-9397-435c-8f95-
4e922c26259e}]
  Oueries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[attributes]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[callforattributes]
  Queries value:
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[restrictedattributes]
                                    HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
  Oueries value:
96b02cfe0d52}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}]
  Queries value:
                                    HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
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:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{edc978d6-4d53-4b2f-a265-
5805674be56811
  Queries value:
                                    HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[attributes]
                                    HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
  Oueries value:
7367fc96ef3c}\shellfolder[callforattributes]
                                    HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
  Oueries value:
7367fc96ef3c}\shellfolder[restrictedattributes]
                                    HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
  Queries value:
7367fc96ef3c}\shellfolder[foldervalueflags]
  Oueries value:
```

```
7367fc96ef3c}]
                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\inprocserver32[]
    Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cqc\} \ d5291c64-7c88-4cqc \ d5291c64
11e3-be65-806e6f6e6963}[data]
    Oueries value:
11e3-be65-806e6f6e6963}[generation]
    Oueries value:
                                                        HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Oueries value:
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
                                                       HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Oueries value:
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
    Queries value:
HKCU \ software \ \verb|microsoft| windows \ \verb|currentversion| explorer \ advanced \ [mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
    Oueries value:
                                                       HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
    Queries value:
                                                       HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
                                                       HKCR\directory[docobject]
    Oueries value:
    Queries value:
                                                       HKCR\folder[docobject]
    Queries value:
                                                        HKCR\allfilesystemobjects[docobject]
    Oueries value:
                                                        HKCR\directory[browseinplace]
    Oueries value:
                                                        HKCR\folder[browseinplace]
                                                        HKCR\allfilesystemobjects[browseinplace]
    Queries value:
    Queries value:
                                                        HKCR\directory[isshortcut]
    Oueries value:
                                                        HKCR\folder[isshortcut]
                                                        HKCR\allfilesystemobjects[isshortcut]
    Queries value:
    Oueries value:
                                                        HKCR\directory[alwaysshowext]
    Queries value:
                                                        HKCR\directory[nevershowext]
    Oueries value:
                                                        HKCR\folder[nevershowext]
                                                        HKCR\allfilesystemobjects[nevershowext]
    Queries value:
    Queries value:
                                                       HKCR \land wow 6432 node \land clsid \land \{75847177 - f077 - 4171 - bd2c - formula \land 
a6bb2164fbd0}\inprocserver32[]
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    Oueries value:
    Queries value:
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[]
    Queries value:
                                                       HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
    Oueries value:
                                                       HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]
    Oueries value:
                                                        HKCR\.exe[content type]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\cmf\config[system]
                                                        HKCR\.exe[]
    Oueries value:
```

Queries value:

HKCR\exefile[docobject]

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

Queries value: HKCR\exefile[browseinplace]

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

Queries value: HKCR\exefile[isshortcut]

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

Queries value: HKCR\exefile[alwaysshowext]

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

Queries value: HKCR\exefile[nevershowext]

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gamm$ 

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma_{bbfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]$ 

Queries value:

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

Queries value:

 $\label{thm:microsoftwindows} HKLM software \noindows \$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{local-software-wow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gamm$ 

Queries value:

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

Queries value:

 $\label{local-loc$ 

folders[desktop]

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{thm:local-basis} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1} b3ea5dc-b587-4786-b4ef-bd1dc332 aeae \footnote{1} [stream resource]$ 

Queries value:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[streamresourcetype]}$ 

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

Queries value: HKCR\exefile[nostaticdefaultverb]

Oueries value: HKCR\exefile\shell[]

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

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

5c9f68572fd1}\inprocserver32[]

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

 $Queries\ value: \\ HKCR\ wow 6432 node \ clsid \ \{76765b11-3f95-4af2-ac9d-46432 node\} \\ Clsid \ (76765b11-3f95-4af2-ac9d-46432 node) \\ Clsid \ (76765b11-3f95-4af2-ac$ 

ea55d8994f1a}\inprocserver32[inprocserver32]

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

ea55d8994f1a}\inprocserver32[]

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

ea55d8994f1a}\inprocserver32[threadingmodel]

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

Queries value:

 $\label{lem:hkcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \ [data]$ 

Queries value:

 $\label{lem:hkcu} HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-11e3-be65-806e6f6e6963\}[generation]}$ 

 $Queries\ value: \\ HKCR\ wow 6432 node \ clsid \ \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\}[]$ 

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

00c04fb6bfc4}\inprocserver32[inprocserver32]

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

00c04fb6bfc4}\inprocserver32[]

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

00c04fb6bfc4}\inprocserver32[threadingmodel]

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

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

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

```
settings[specialfolderscachesize]
```

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

settings[specialfolderscachesize]

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

explorer\main\featurecontrol\feature\_protocol\_lockdown[6f2064e626e4383a5d8a9c0bdb8e9ddf.exe]

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

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

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

settings\zones\0[1806]

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

settings\zones\0[1806]

Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[52f82e4b]

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

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

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

Oueries value:

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

Oueries value:

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

Queries value:

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

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

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]

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

folders[cache]

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

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

Queries value:

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the constr$ 

Queries value: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\compatibility32[conhost]|\\$ 

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

HKCU\console[screencolors] Queries value: Queries value: HKCU\console[popupcolors] Oueries value: HKCU\console[insertmode] HKCU\console[quickedit] Queries value: Oueries value: HKCU\console[codepage] HKCU\console[screenbuffersize] Oueries value: HKCU\console[windowsize] Oueries value: HKCU\console[windowposition] Queries value: Oueries value: HKCU\console[fontsize] Queries value: HKCU\console[fontfamily] Oueries value: HKCU\console[fontweight] Oueries value: HKCU\console[facename] HKCU\console[cursorsize] Oueries value:

Queries value: HKCU\console[historybuffersize]
Queries value: HKCU\console[numberofhistorybuffers]

Queries value: HKCU\console[historynodup] Oueries value: HKCU\console[colortable001 Queries value: HKCU\console[colortable01] HKCU\console[colortable02] Oueries value: HKCU\console[colortable03] Oueries value: HKCU\console[colortable04] Oueries value: HKCU\console[colortable05] Queries value: Queries value: HKCU\console[colortable06] Oueries value: HKCU\console[colortable07] HKCU\console[colortable08] Queries value: Queries value: HKCU\console[colortable09] HKCU\console[colortable10] Oueries value: HKCU\console[colortable11] Oueries value: Queries value: HKCU\console[colortable12] Oueries value: HKCU\console[colortable13] Queries value: HKCU\console[colortable14] Queries value: HKCU\console[colortable15] Queries value: HKCU\console[loadconime] HKCU\console[extendededitkey] Oueries value:

Queries value: HKCU\console[worddelimiters]
Queries value: HKCU\console[trimleadingzeros]
Queries value: HKCU\console[enablecolorselection]

Queries value: HKCU\console[scrollscale]

Queries value: HKLM\system\currentcontrol\set\control\nls\codepage\eudccoderange[1252] Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]

Queries value:

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [turnoff spianimations]$ 

HKCU\console[extendededitkeycustom]

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

```
Oueries value:
                                                                              HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]
     Oueries value:
                                                                              HKLM\software\wow6432node\microsoft\command processor[defaultcolor]
     Oueries value:
                                                                              HKLM\software\wow6432node\microsoft\command processor[completionchar]
     Queries value:
                                                                              HKLM\software\wow6432node\microsoft\command
processor[pathcompletionchar]
     Queries value:
                                                                             HKLM\software\wow6432node\microsoft\command processor[autorun]
     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]
     Oueries value:
                                                                              HKCU\software\microsoft\command processor[completionchar]
     Oueries value:
     Queries value:
                                                                              HKCU\software\microsoft\command processor[pathcompletionchar]
     Oueries value:
                                                                              HKCU\software\microsoft\command processor[autorun]
     Oueries value:
                                                                             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[tasklist]
                                                                             HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
     Queries value:
     Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
     Queries value:
                                                                             HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
                                                                             HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
     Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
     Queries value:
                                                                             HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[]
                                                                             HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
     Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                                                                             HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| wbem \verb|\cimom[logging directory]|
     Queries value:
     Queries value:
                                                                              HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus wbem \setminus cimom[log file max size] \\
     Queries value:
                                                                              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
                                                                             HKLM\software\microsoft\ole[maximumallowedallocationsize]
     Oueries value:
                                                                              HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
     Queries value:
00c04fb68820}\proxystubclsid32[]
                                                                             HKCR \setminus wow6432 \\ node \\ clsid \\ \{7c857801-7381-11cf-884d-00aa004b2e24\}[]
     Queries value:
                                                                              HKCR \setminus wow 6432 \\ node \setminus clsid \setminus \{7c857801 - 7381 - 11cf - 884d - 11cf - 11cf
     Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                                                             HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
     Oueries value:
00aa004b2e24}\inprocserver32[]
                                                                             HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
     Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                                                                             HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32[]
                                                                             HKCR \setminus wow6432 \\ node \\ clsid \\ \{674b6698 - ee92 - 11d0 - ad71 - 00c04fd8fdff\}[]
     Oueries value:
                                                                              HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
     Queries value:
00c04fd8fdff}\inprocserver32[inprocserver32]
                                                                             HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
     Queries value:
00c04fd8fdff}\inprocserver32[]
                                                                             HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
     Queries value:
00c04fd8fdff}\inprocserver32[threadingmodel]
     Queries value:
                                                                              HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
     Oueries value:
                                                                              HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
     Queries value:
                                                                             HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
                                                                              HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
     Oueries value:
     Oueries 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]
                                                                             HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
     Oueries value:
00aa003240c7}\proxystubclsid32[]
                                                                             HKCR \wow6432 node \clsid \d68af00a-29cb-43fa-8504-ce99a996d9ea \clsid \clsid \d68af00a-29cb-43fa-8504-ce99a996d9ea \clsid \cl
     Queries value:
     Oueries value:
                                                                              HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
                                                                             HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
     Queries value:
ce99a996d9ea}\inprocserver32[]
     Queries value:
                                                                             HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
                                                                             HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
     Oueries value:
                                                                             HKCR\wow6432 node\clsid\ef{e7d35cfa-348b-485e-b524-b524-b6485e-b524-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6
     Queries value:
252725d697ca}\inprocserver32[inprocserver32]
                                                                             HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
    Queries value:
252725d697ca}\inprocserver32[]
     Queries value:
                                                                             HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6486e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6485e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b6486e-b
252725d697ca}\inprocserver32[threadingmodel]
     Queries value:
                                                                             HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
00000000001}\proxystubclsid32[]
                                                                             HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
     Oueries value:
     Oueries value:
                                                                             HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
                                                                             HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1cad8c-2dab-11d2-b604-1b1c
     Oueries value:
00104b703efd}\inprocserver32[]
     Oueries value:
                                                                             HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
     Oueries value:
                                                                             HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32[]
                                                                             HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
     Oueries value:
00104b703efd}\proxystubclsid32[]
```

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

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

00c04fb68820}\inprocserver32[inprocserver32]

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

00c04fb68820}\inprocserver32[]

00c04fb68820}\inprocserver32[threadingmodel]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

 $\label{thm:condition} \mbox{Value changes:} \qquad \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\label{thm:condition}} \mbox{\sc microsoft\windows\currentversion\currentvers$ 

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\history[cacheprefix]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]