# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 228, Task ID: 912

Task ID: 912 Risk Level:

Date Processed: 2016-04-28 13:12:25 (UTC)

Processing Time: 61.19 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe"

Sample ID: Type: basic admin Owner:

5707475dc2b4470cb1ec56f978fbe4bd Label:

Date Added: 2016-04-28 12:45:13 (UTC) PE32:win32:gui File Type:

File Size: 368256 bytes

5707475dc2b4470cb1ec56f978fbe4bd MD5:

599cb9421166c30c3dc09c2d76376f093290c908abd0bb2a4214cd03f9e5ab3c SHA256:

Description: None

## Pattern Matching Results

2 PE: Nonstandard section

5 Packer: UPX

5 PE: Contains compressed section

## Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Packer:

#### Process/Thread Events

Creates process: C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe

["C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe"]

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

Creates semaphore:

\Sessions\1\BaseNamedObjects\5707475dc2b4470cb1ec56f978fbe4bd.exeYkvnYWiq

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1 Creates mutex: Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

Creates event: \KernelObjects\MaximumCommitCondition

Creates semaphore:  $\verb|\Sessions| 1 \\ BaseNamedObjects \\ INI-5707475dc2b4470cb1ec56f978fbe4bd.data| \\$ 

Creates semaphore: \Sessions\1\BaseNamedObjects\GR\_FileChecker

Creates semaphore: \Sessions\1\BaseNamedObjects\GR0

Creates semaphore: \Sessions\1\BaseNamedObjects\GR\_FlushingList Creates semaphore: \Sessions\1\BaseNamedObjects\GR\_Write

Creates semaphore: \Sessions\1\BaseNamedObjects\GR\_GErrMsg \Sessions\1\BaseNamedObjects\GR1 Creates semaphore:

Creates semaphore: \Sessions\1\BaseNamedObjects\GR2 Creates semaphore: \Sessions\1\BaseNamedObjects\GR3 \Sessions\1\BaseNamedObjects\GR4 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR5 Creates semaphore: \Sessions\1\BaseNamedObjects\GR6 \Sessions\1\BaseNamedObjects\GR7 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR8 Creates semaphore: \Sessions\1\BaseNamedObjects\GR9 \Sessions\1\BaseNamedObjects\GR10 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR11

Creates semaphore: \Sessions\1\BaseNamedObjects\GR12 \Sessions\1\BaseNamedObjects\GR13 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR14 Creates semaphore: \Sessions\1\BaseNamedObjects\GR15

\Sessions\1\BaseNamedObjects\GR16 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR17 \Sessions\1\BaseNamedObjects\GR18 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR19 \Sessions\1\BaseNamedObjects\GR20 Creates semaphore:

Creates semaphore: \Sessions\1\BaseNamedObjects\GR21 Creates semaphore: \Sessions\1\BaseNamedObjects\GR22 Creates semaphore: \Sessions\1\BaseNamedObjects\GR23 Creates semaphore: \Sessions\1\BaseNamedObjects\GR24 Creates semaphore: \Sessions\1\BaseNamedObjects\GR25

\Sessions\1\BaseNamedObjects\GR26 Creates semaphore: \Sessions\1\BaseNamedObjects\GR27 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR28

\Sessions\1\BaseNamedObjects\GR29

\Sessions\1\BaseNamedObjects\GR30 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR31 \Sessions\1\BaseNamedObjects\GR32 Creates semaphore: \Sessions\1\BaseNamedObjects\GR33 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR34 Creates semaphore: \Sessions\1\BaseNamedObjects\GR36 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR37 Creates semaphore: \Sessions\1\BaseNamedObjects\GR38 Creates semaphore: \Sessions\1\BaseNamedObjects\GR39 \Sessions\1\BaseNamedObjects\GR40 Creates semaphore: Creates semaphore:  $\Sessions\1\BaseNamedObjects\GR41$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR42 \Sessions\1\BaseNamedObjects\GR43 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR44 Creates semaphore: \Sessions\1\BaseNamedObjects\GR45 \Sessions\1\BaseNamedObjects\GR46 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR47 Creates semaphore: \Sessions\1\BaseNamedObjects\GR48 Creates semaphore: \Sessions\1\BaseNamedObjects\GR49 Creates semaphore: \Sessions\1\BaseNamedObjects\GR50 Creates semaphore: \Sessions\1\BaseNamedObjects\GR51 \Sessions\1\BaseNamedObjects\GR52 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR53 Creates semaphore: \Sessions\1\BaseNamedObjects\GR54 Creates semaphore: \Sessions\1\BaseNamedObjects\GR55 Creates semaphore: \Sessions\1\BaseNamedObjects\GR56 Creates semaphore: \Sessions\1\BaseNamedObjects\GR57 Creates semaphore: \Sessions\1\BaseNamedObjects\GR58 Creates semaphore: \Sessions\1\BaseNamedObjects\GR59 Creates semaphore: \Sessions\1\BaseNamedObjects\GR60 \Sessions\1\BaseNamedObjects\GR61 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR62 Creates semaphore: \Sessions\1\BaseNamedObjects\GR63 \Sessions\1\BaseNamedObjects\GR64 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR66 Creates semaphore: \Sessions\1\BaseNamedObjects\GR67 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR68 Creates semaphore: \Sessions\1\BaseNamedObjects\GR69 \Sessions\1\BaseNamedObjects\GR70 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR71 \Sessions\1\BaseNamedObjects\GR72 Creates semaphore: \Sessions\1\BaseNamedObjects\GR73 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR74 \Sessions\1\BaseNamedObjects\GR75 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR76 Creates semaphore: \Sessions\1\BaseNamedObjects\GR77 Creates semaphore: \Sessions\1\BaseNamedObjects\GR78 Creates semaphore: \Sessions\1\BaseNamedObjects\GR79 \Sessions\1\BaseNamedObjects\GR80 Creates semaphore: \Sessions\1\BaseNamedObjects\GR81 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR82 \Sessions\1\BaseNamedObjects\GR83 Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR88  $\verb|\Sessions|1\\BaseNamedObjects|GR89|$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR90 Creates semaphore: \Sessions\1\BaseNamedObjects\GR91 Creates semaphore: \Sessions\1\BaseNamedObjects\GR92 Creates semaphore: \Sessions\1\BaseNamedObjects\GR93 \Sessions\1\BaseNamedObjects\GR94 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR95 Creates semaphore: \Sessions\1\BaseNamedObjects\GR96 Creates semaphore: \Sessions\1\BaseNamedObjects\GR97 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-5707475dc2b4470cb1ec56f978fbe4bd.data0

# File System Events

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Creates: C:\Users

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

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

 $\label{lem:condition} Creates: $C:\Users\land Admin\land ppData\Roaming\GetRightToGo. $C:\Users\land Admin\land ppData\Roaming\GetRightToGo. $$C:\Users\land Admin\Admin\GetRightToGo. $$C:\Users\Admin\Admin\GetRightToGo. $$C:\Users\Admin\Adm$ 

Creates:

```
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data
 Creates
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data0
                         C:\Windows\Prefetch\5707475DC2B4470CB1EC56F978FBE-33C1147B.pf
 Opens:
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\System32\sechost.dll
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe.Local\
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens:
                         C:\windows\temp\oledlg.dll
 Opens:
                         C:\Windows\System32\oledlg.dll
                         C:\windows\temp\Secur32.dll
 Opens:
 Opens:
                         C:\Windows\System32\secur32.dll
 Opens:
                         C:\windows\temp\SSPICLI.DLL
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\windows\temp\WINSPOOL.DRV
 Opens:
                         C:\Windows\System32\winspool.drv
 Opens:
                         C:\Windows\System32\imm32.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\Windows\System32\uxtheme.dll
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe.2.Manifest
 Opens:
 Opens:
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe.3.Manifest
 Opens:
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe.Config
                         C:\Windows\Temp\5707475dc2b4470cb1ec56f978fbe4bd.exe
 Opens:
 Opens:
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bd.exe.1000.Manifest
 Opens:
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bdENU.dll
 Opens:
                         C:\windows\temp\5707475dc2b4470cb1ec56f978fbe4bdL0C.dll
 Opens:
                         C:\
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Windows\System32\tzres.dll
 Opens:
                         C:\Windows\System32\en-US\tzres.dll.mui
 Opens:
                         C:\Windows\Fonts\tahoma.ttf
 Opens:
                         C:\windows\temp\dwmapi.dll
 Opens:
                         C:\Windows\System32\dwmapi.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
                         C:\Windows\Fonts\StaticCache.dat
 Opens:
 Opens:
                         C:\Windows\System32\shell32.dll
 Opens:
                         C:\Users\Admin\Desktop
 Opens:
                         C:\Windows\System32\propsys.dll
 Opens:
                         C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db|
 Opens:
                         C:\windows\temp\ntmarta.dll
 Opens:
                         C:\Windows\System32\ntmarta.dll
 Opens:
                         4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
                        C:\Users\desktop.ini
 Opens:
 Opens:
                        C:\Users
 Opens:
                        C:\Users\Admin
                        C:\Users\Admin\Desktop\desktop.ini
 Opens:
 Opens:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Users\Admin\AppData\Roaming
 Opens:
                         C:\Users\Admin\AppData
                         C:\Users\Admin\AppData\Roaming\GetRightToGo
 Opens:
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data
 Opens:
                         C:\Windows\Temp
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data0
                        C:\Users\Admin\Desktop\Downloads\
 Opens:
 Opens:
                         C:\Users\Admin\Documents
                         C:\Users\Admin\Documents\desktop.ini
 Opens:
 Opens:
                        C:\Users\Public\Desktop
 Opens:
                        C:\Users\Public\desktop.ini
 Opens:
                        C:\Users\Public
 Opens:
                         C:\Users\Public\Desktop\desktop.ini
                         C:\Windows\Fonts\sserife.fon
 Opens:
 Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data
 Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data0
 Reads from:
                        C:\Windows\Fonts\StaticCache.dat
 Reads from:
                         C:\Users\desktop.ini
 Reads from:
                         C:\Users\Admin\Desktop\desktop.ini
                         C:\Windows\Temp\5707475dc2b4470cb1ec56f978fbe4bd.exe
 Reads from:
 Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data
 Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\5707475dc2b4470cb1ec56f978fbe4bd.data0
 Reads from:
                         C:\Users\Admin\Documents\desktop.ini
```

Reads from: C:\Users\Public\desktop.ini C:\Users\Public\Desktop\desktop.ini Reads from:

## Windows Registry Events

HKCU\software\headlight Creates key: Creates key: HKCU\software\headlight\getrighttogo Creates key: HKCU\software\headlight\getrighttogo\sharedconfig Creates key: HKCU\software\headlight\getrighttogo\customizedapps Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\terminal server Opens kev: HKLM\svstem\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\ Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration HKLM\software\policies\microsoft\mui\settings Opens kev: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration Opens key: Opens key: HKCU\control panel\desktop Opens key: HKCU\control panel\desktop\muicached HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\ Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\svstem\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: HKLM\software\microsoft\ole Opens kev: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\microsoft\oleaut Opens key: HKCU\software\classes\ HKCU\software\classes\clsid Opens kev: Opens key: HKCR\clsid Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\network Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32 HKLM\system\currentcontrolset\control\nls\customlocale Opens key: Opens kev: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr Opens key: HKLM\system\currentcontrolset\control\computername Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: HKLM\system\setup HKLM\system\currentcontrolset\control\nls\locale Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key: HKLM\software\microsoft\ctf\compatibility\5707475dc2b4470cb1ec56f978fbe4bd.exe HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-Opens key: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens key: HKLM\software\microsoft\ctf\ Opens key: HKLM\software\microsoft\ctf\knownclasses Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0 HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows 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\0f9f3ff3 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries Opens kev: 

Opens kev:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
    Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ parameters \ protocol\_catalog\_entries \ protocol\_catalog \ parameters \ parameters
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
    Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col\_catalog 9 \setminus catalog\_entries \setminus 0000000000011
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000012
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000013
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
    Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000016) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000017
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000018
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
    Opens key:
HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ name space\_catalog 5 \ 0000000c
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
    Opens key:
                                                              HKLM\software\microsoft\windows\currentversion\policies\explorer
    Opens kev:
Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions
    Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-
b029-7fe99a87c641}
    Opens kev:
b029-7fe99a87c641}\propertybag
                                                              HKCU\software\microsoft\windows\currentversion\explorer
    Opens key:
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
    Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current \vee explorer \setminus session in follows \cap the following of the fol
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
    Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus known folders ettings
```

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{20d04fe0-development \ explorer \ explorer \ and \ explorer \ e$ Opens key:

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens kev: HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key:

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

Opens key:

11e3-b3bc-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: HKLM\software\policies\microsoft\windows\explorer HKCU\software\policies\microsoft\windows\explorer Opens key:

HKLM\software\microsoft\com3 Opens key:

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

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\progid

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

b8dc300d9f9d}\inprocserver32

Opens key:  $HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32$ 

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

b8dc300d9f9d}\inprochandler32

Opens key:  $HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\) in prochandler 32$ 

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 4$ Opens kev:

b8dc300d9f9d}\inprochandler

Opens key:  $HKCR \verb|\clsid|{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} \verb|\inprochandler| \\$  $HKLM \verb|\system| current controlset \verb|\control| lsa \verb|\accessproviders| \\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\ldap Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

Opens key:

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

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

Opens key: HKCR\directorv\curver

Opens key: HKCR\directory\

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

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

Opens key: HKCR\folder

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

HKCR\folder\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

HKCR\folder\docobject Opens key:

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

HKCR\allfilesystemobjects\docobject Opens key:

HKCU\software\classes\directorv\browseinplace Opens kev:

Opens key: HKCR\directory\browseinplace

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

Opens key: HKCR\folder\browseinplace

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

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

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key:  ${\it HKLM \ } software \ \\ microsoft \ \\ windows \ \\ current version$ 

Opens key: HKLM\software\microsoft\rpc

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

Opens key: HKCU\software

a03a-e3ef65729f3d}

Opens key:

a03a-e3ef65729f3d}\propertybag

11e3-b3bc-806e6f6e6963}\

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ (ab 3ea 5dc - b 587 - 4786 - b 587 - b 587$ b4ef-bd1dc332aeae}

Opens key:

b4ef-bd1dc332aeae}\propertybag

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens kev:

adb4-6c85480369c7}

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ fdd 39 ad 0-238 f-46 af-46 af-4$ 

 $adb4-6c85480369c7 \} \verb|\propertybag|$ 

Opens key: HKCU\software\classes\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder

Opens key: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-

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

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-

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

Opens key:

afef-f87ef2e6ba25}

Opens kev:

afef-f87ef2e6ba25}\propertybag

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

folders

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms sans serif

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

manager[cwdillegalindllsearch]

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

Queries value:

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

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

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

Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrol\sorting\versions[]

Queries value: HKLM\system\currentcontrol\set\control\session manager[safedllsearchmode]

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

nt\currentversion\compatibility32[5707475dc2b4470cb1ec56f978fbe4bd]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]

Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]

Queries value:

 ${\tt HKLM \ } {\tt system \ } {\tt computername \ } {\tt active computername \ } {\tt computername \ } {\tt in \ } {\tt computername \ } {$ 

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

Queries value: HKLM\system\currentcontrol\set\control\nls\locale[00000409]

Queries value: HKLM\system\currentcontrol\set\control\nls\language groups[1]

Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]

Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]

HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\datastore\_v1.0[disable] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0[datafilepath] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane3] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane4]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane5]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows

```
nt\currentversion\languagepack\surrogatefallback[plane8]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
 Queries value:
                      HKLM\software\microsoft\windows
nt\current version \verb|\languagepack\surrogatefallback[plane10]|
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000003[packedcatalogitem]
 Oueries value:
Oueries value:
Queries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000007 \ [packed catalog item]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000018[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]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ set alog\_entries \ (0000000000001[version]) \ details \ de$ 

Oueries value:

Queries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo]

  Oueries 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\0000000000002[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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 0000000000003 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid] Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names family] \\ Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo]
  Queries value:
- $\label{lem:hklmsystem} Hklm\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo]\queries\value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Queries value:
- $\label{lem:hklm} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]\\ Oueries\ value: \begin{tabular}{ll} Color of the color of$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
- $\label{local-parameters} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000005[storesserviceclassinfo]\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
  Oueries value:

Oueries value:

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[version]
Queries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \namespace\_catalog5 \catalog3 \cat$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32spincount]

Queries value:

b029-7fe99a87c641}[category]

Queries value:

Queries value:

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

Oueries value

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value

Queries value

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folder$ 

Oueries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[streamresource]}$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescript$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[local redirectonly]$ 

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \end{are the lemma of the label} In the label lemma of the label lem$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (b4bfcc3a-db2c-424c-b029-7fe99a87c641) \ [precreate]$ 

Queries value

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescript$ 

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosof$ 

Queries value

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}\[attributes\]$ 

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsof$ 

Queries value:

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

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

folders[desktop]

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

08002b30309d}\shellfolder[attributes]

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

08002b30309d}\shellfolder[callforattributes]

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

08002b30309d}\shellfolder[restrictedattributes]

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

```
08002b30309d}\shellfolder[wantsfordisplay]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
   Oueries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
   Oueries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
   Queries value:
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                                 HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus monenum [\{20d04fe0-3aea-1069-a2d8-microsoft\}] + (20d04fe0-3aea-1069-a2d8-microsoft) + (20d04fe0-3aea-1069-a2d8-mi
08002b30309d}1
11e3-b3bc-806e6f6e6963}[data]
11e3-b3bc-806e6f6e6963}[generation]
                                                 HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Queries value:
                                                 HKLM\software\microsoft\com3[com+enabled]
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Queries value:
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
   Oueries value:
   Queries value:
                                                 HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Queries value:
                                                 HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                                 HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Oueries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Oueries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Oueries value:
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Queries value:
\label{thm:limit} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{thm:limits} advanced \cite{thm:limits}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
   Queries value:
                                                 HKCR\directory[docobject]
```

Queries value: HKCR\folder[docobject]

 $\label{lem:condition} Queries \ value: \qquad \qquad \mathsf{HKCR} \ all filesystem objects [docobject]$ 

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

Queries value: HKCR\allfilesystemobjects[browseinplace]

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

Queries value: HKCR\allfilesystemobjects[isshortcut]

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

Queries value: HKCR\allfilesystemobjects[nevershowext]

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

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

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

Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[useloadimage]
Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[doxpthemes]
Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'aeb685db-65f9-4cf6-a03a-e3ef65729f3d \ '[category]$ 

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'ab685 db-65 f9-4 cf6-a03a-e3ef65729 f3d \ [name]$ 

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [security]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hkklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hkklm} a be 685db-65f9-4cf6-a03a-e3ef65729f3d \cal{lem:hkklm} [precreate]$ 

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[stream]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[appdata]

Queries value:

 $\label{thm:local-continuity} HKCU software \\ \mbox{microsoft} \mbox{windows} \mbox{currentversion} \mbox{explorer} \mbox{mountpoints2} \mbox{cpc} \mbox{volume} \mbox{69d250e3-6c18-11e3-b3bc-806e6f6e6963} \mbox{[data]}$ 

Queries value:

 $\label{lem:hkcu} HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e3-6c18-11e3-b3bc-806e6f6e6963\}[generation]}$ 

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [category]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'endows \ 'en$ 

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value

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

Queries value:

 $HKLM \ software \ `microsoft \ 'unidows \ 'current version \ 's the abded-b587-4786-b4ef-bd1dc332aeae \ [stream resource type]$ 

Oueries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [local redirectonly]$ 

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'unidows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]$ 

Queries value:

 $\label{local-basis} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream]}$ 

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[folder typeid]$ 

Queries value:

Queries value:  $HKCU \setminus software \in \windows \subset \windows$ 

Queries value:

HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]

 $\label{lem:policies} $$\operatorname{Queries value:}$ HKLM\software\policies\microsoft\windows\system[copyfilechunksize] $$\operatorname{HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]} $$$ 

Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[debug]

Queries value:

 $\label{local-continuous} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\cite{Continuous}\$ 

Queries value:

 $\label{thm:local-prop} $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7\}[name]$$$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{fdd39ad0-238f-46af-adb4-6c85480369c7\} \ [parent folder]$ 

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} In the label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwaremicrosoftwarem$ 

Queries value:

```
adb4-6c85480369c7}[relativepath]
    Oueries value:
adb4-6c85480369c7}[parsingname]
    Oueries value:
adb4-6c85480369c7}[infotip]
    Oueries value:
adb4-6c85480369c7}[localizedname]
    Oueries value:
adb4-6c85480369c7}[icon]
    Oueries value:
adb4-6c85480369c7}[security]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ fdd 39 ad 0-238 f-46 af-46 
adb4-6c85480369c7}[streamresource]
    Queries value:
adb4-6c85480369c7}[streamresourcetype]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ fdd 39 ad 0-238 f-46 af-46 
adb4-6c85480369c7}[localredirectonly]
    Queries value:
adb4-6c85480369c7}[roamable]
    Oueries value:
adb4-6c85480369c7}[precreate]
    Queries value:
adb4-6c85480369c7}[stream]
    Oueries value:
adb4-6c85480369c7}[publishexpandedpath1
    Queries value:
adb4-6c85480369c7}[attributes]
    Oueries value:
adb4-6c85480369c7}[foldertypeid]
    Queries value:
HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ fdd 39 ad 0-238 f-46 af-46 af
adb4-6c85480369c7}[initfolderhandler]
    Queries value:
                                                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders[personal]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[attributes]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
    Oueries value:
5595fe6b30ee}\shellfolder[callforattributes]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[restrictedattributes]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[wantsfordisplay]
    Queries value:
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[hidefolderverbs]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[usedrophandler]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[wantsforparsing]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[queryforoverlay]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[mapnetdriveverbs]
    Queries value:
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[queryforinfotip]
    Queries value:
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[hideinwebview]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[hideondesktopperuser]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
    Queries value:
5595fe6b30ee}\shellfolder[wantsaliasednotifications]
    Queries value:
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
                                                         HKCR\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
```

5595fe6b30ee}\shellfolder[nofilefolderjunction]

5595fe6b30ee}\shellfolder[pintonamespacetree]

Queries value:

Queries value:

HKCR\clsid\{59031a47-3f72-44a7-89c5-

HKCR\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[hasnavigationenum]

Queries value:

5595fe6b30ee}]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [category]$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [name]$ 

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[parent folder]$ 

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [description]$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [relative path]$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [parsing name]$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[infotip]$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[localized name]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[icon]}$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [security]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ for earlier \ folder \ folder$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [stream resource type]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ flocal redirect \ folder \ fold$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [roamable]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [precreate]$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [stream] \\$ 

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$ 

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}[foldertypeid]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}\initfolderhandlerl

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

folders[common desktop]

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[5707475dc2b4470cb1ec56f978fbe4bd]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[busypause]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecache]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecachekb]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[rollback]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[dotgetright]