# Malware Analysis Appliance by Blue Coat Systems, Inc.

### Task Details

Host: mag2, Sample ID: 13, Task ID: 51

Task ID: 51 Risk Level:

Date Processed: 2016-04-28 12:47:06 (UTC)

Processing Time: 63.48 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\a58d51951bbc071eb0828eab9d9b464d.exe"

Sample ID: 13 Type: basic admin Owner:

a58d51951bbc071eb0828eab9d9b464d Label:

Date Added: 2016-04-28 12:44:51 (UTC)

PE32:win32:gui File Type: File Size: 368264 bytes

a58d51951bbc071eb0828eab9d9b464d MD5:

c2ca2797e54c2320b5c90aa49d2839ea89a6dd2c8c38323ded84824a525cd9c0 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\a58d51951bbc071eb0828eab9d9b464d.exe

["C:\windows\temp\a58d51951bbc071eb0828eab9d9b464d.exe" ]

### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

\Sessions\1\BaseNamedObjects\a58d51951bbc071eb0828eab9d9b464d.exepzJnl5TE 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: \Sessions\1\BaseNamedObjects\INI-a58d51951bbc071eb0828eab9d9b464d.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 Creates semaphore: \Sessions\1\BaseNamedObjects\GR16 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 Creates semaphore: \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: \Sessions\1\BaseNamedObjects\GR34 Creates semaphore: 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:  $\Sessions\1\BaseNamedObjects\GR65$ \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:  $\verb|\Sessions|1\BaseNamedObjects|| GR98||$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-a58d51951bbc071eb0828eab9d9b464d.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

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

Creates:

```
Creates
C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data0
                         C:\Windows\Prefetch\A58D51951BBC071EB0828EAB9D9B4-89172D41.pf
 Opens:
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\Windows\System32\sechost.dll
                         C:\windows\temp\a58d51951bbc071eb0828eab9d9b464d.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
 Opens:
                         C:\windows\temp\Secur32.dll
 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\a58d51951bbc071eb0828eab9d9b464d.exe.2.Manifest
 Opens:
 Opens:
                         C:\windows\temp\a58d51951bbc071eb0828eab9d9b464d.exe.3.Manifest
 Opens:
                         C:\windows\temp\a58d51951bbc071eb0828eab9d9b464d.exe.Config
 Opens:
                         C:\Windows\Temp\a58d51951bbc071eb0828eab9d9b464d.exe
 Opens:
                         C:\windows\temp\a58d51951bbc071eb0828eab9d9b464d.exe.1000.Manifest
 Opens:
                         C:\windows\temp\a58d51951bbc071eb0828eab9d9b464dENU.dll
 Opens:
                         C:\windows\temp\a58d51951bbc071eb0828eab9d9b464dL0C.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.dl1
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
 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:
                         C:\Windows\System32\en-US\setupapi.dll.mui
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
                         C:\Users\desktop.ini
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin
 Opens:
 Opens:
                         C:\Users\Admin\Desktop\desktop.ini
 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\a58d51951bbc071eb0828eab9d9b464d.data
 Opens:
                         C:\Windows\Temp
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data0
                         C:\Users\Admin\Desktop\Downloads\
 Opens:
 Opens:
                         C:\Windows\System32\en-US\user32.dll.mui
                         C:\Users\Admin\Documents
 Opens:
 Opens:
                         C:\Users\Admin\Documents\desktop.ini
 Opens:
                         C:\Users\Public\Desktop
 Opens:
                         C:\Users\Public\desktop.ini
 Opens:
                         C:\Users\Public
                         C:\Users\Public\Desktop\desktop.ini
 Opens:
 Opens:
                         C:\Windows\Fonts\sserife.fon
 Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data
 Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data0
 Reads from:
                         C:\Windows\Fonts\StaticCache.dat
 Reads from:
                         C:\Users\desktop.ini
 Reads from:
                         C:\Users\Admin\Desktop\desktop.ini
 Reads from:
                         C:\Windows\Temp\a58d51951bbc071eb0828eab9d9b464d.exe
 Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data
 Reads from:
C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data0
```

C:\Users\Admin\AppData\Roaming\GetRightToGo\a58d51951bbc071eb0828eab9d9b464d.data

Reads from: C:\Users\Admin\Documents\desktop.ini

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

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

# Windows Registry Events

Creates key: HKCU\software\headlight

Creates key: HKCU\software\headlight\getrighttogo

Creates key: HKCU\software\headlight\getrighttogo\sharedconfig
Creates key: HKCU\software\headlight\getrighttogo\customizedapps
Opens key: HKLM\system\currentcontrol\set\control\session manager
Opens key: HKLM\system\currentcontrol\set\control\terminal server
Opens key: HKLM\system\currentcontrol\set\control\safeboot\option
Opens key: HKLM\system\currentcontrol\set\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

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

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\microsoft\windows\currentversion\sidebyside

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$ 

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

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

Opens key: HKLM\software\microsoft\ole

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

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: 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

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:

 $\label{lem:hklmsoftwaremicrosoft} This is the state of the compatibility and the state of the$ 

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

 $nt\current version\language pack\datastore\_v1.0$ 

Opens key: HKLM\software\microsoft\windows 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:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus appid\_catalog \setminus 34453c25$ 

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9$ 

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000019

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens kev:

Opens key:

Opens key:

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

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000010 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000011 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000013 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000014 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000016 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000017 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000018

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

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\0000000c Opens kev:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000004 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000005 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006 HKLM\software\microsoft\windows\currentversion\policies\explorer Opens kev:

Opens key:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' shell compatibility \ 'applications' a 58d 51951bbc 071eb 0828eab 9d9b 464d. exemple the shell compatibility is a simple of the shell compatibility in the shell compatibility is a shell compatibility of the shell compatibility is a shell compatibility of the shell compatibility is a shell compatibility of the shell compatibility of the$ Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-

b029-7fe99a87c641}

Opens kev:

b029-7fe99a87c641}\propertybag

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

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

Opens kev:

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

folders Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-Opens kev:

08002b30309d}\shellfolder

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

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

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

Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta, for explorer \setminus clsid \setminus \{20d04f$ 

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

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

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ (explorer \ mountpoints 2 \ cpc \ volume) \ (explorer \ mountpoints 2 \ cpc) \ volume) \ (explorer \ mountpoints 2 \ cpc) \ volume) \ (explorer \ mountpoints 2 \ cpc) \ volume) \ (explorer \ mountpoints 2 \ cpc) \ volume) \ (explorer \ mountpoints 2 \ cpc) \ (explorer \$ 

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

Opens key: HKLM\software\microsoft\com3

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

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

b8dc300d9f9d}\treatas

 $\label{lem:continuous} Opens~key: $$ HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$$ Opens~key: $$ HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas$$ Opens~key: $$ Opens~ke$ 

b8dc300d9f9d}\progid

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

 Opens key:
 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}\inprochandler32

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

b8dc300d9f9d}\inprochandler

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
Opens key: HKLM\system\currentcontrol\set\control\lsa\accessproviders
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows\currentversion\setup

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

Opens key: HKLM\software\microsoft\rpc

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

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced$ 

Opens key:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \shell registered applications \urlass ociations \directory \shell \noindent \noindent$ 

Opens key:

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

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

Opens key:  $\label{local-opens} \begin{tabular}{ll} HKCU \software \classes \directory \shellex \directory \directory$ 

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

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

Opens key: HKCR\folder\browseinplace

 $Opens\ key: \\ HKCU \ software \ classes \ all file system objects \ browsein place$ 

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

Opens key: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key: HKCU\software

Opens key:

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

иза-езеть: Opens kev:

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

Opens kev:

 $\label{thm:back} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \{69d250e3-6c18-11e3-b3bc-806e6f6e6963} \label{thm:back} \\ \label{thm:back}$ 

Opens kev:

 $\label{thm:local-continuity} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b587-4786-b587-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-4786-b687-47$ 

```
b4ef-bd1dc332aeae}
  Opens kev:
b4ef-bd1dc332aeae}\propertybag
                                   HKLM\software\policies\microsoft\windows\system
  Opens kev:
  Opens key:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-
adb4-6c85480369c7}
  Opens kev:
adb4-6c85480369c7}\propertybag
                                   HKCU\software\classes\clsid\{59031a47-3f72-44a7-89c5-
  Opens kev:
5595fe6b30ee}\shellfolder
  Opens key:
                                    HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder
                                   HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
  Onens key:
3f72-44a7-89c5-5595fe6b30ee}\shellfolder
  Opens key:
                                   3f72-44a7-89c5-5595fe6b30ee}\shellfolder
afef-f87ef2e6ba25}
  Opens key:
afef-f87ef2e6ba25}\propertybag
                                   HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Opens key:
folders
                                   HKLM\software\microsoft\windows
  Opens kev:
nt\currentversion\languagepack\surrogatefallback\ms sans serif
  Queries value:
                                   HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
                                    HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
                                   HKCU\control panel\desktop[preferreduilanguages]
  Oueries value:
  Oueries value:
                                   HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                    HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\compatibility32[a58d51951bbc071eb0828eab9d9b464d]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Oueries value:
                                   HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:
                                   HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                                    HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Oueries value:
  Oueries value:
                                    HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-usl
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:
                                    HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Oueries value:
HKLM\system\currentcontrolset\control\computername[computername]
  Oueries value:
                                    HKLM\system\setup[oobeinprogress]
                                    HKLM\system\setup[systemsetupinprogress]
  Queries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\language groups[1]
                                    HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
  Queries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Oueries 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]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
  Oueries value:
```

HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane3] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane4] Oueries value: HKLM\software\microsoft\windows  $\verb|nt\currentversion\language| pack\surrogatefallback[plane5]|$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane7]

```
Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                      HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane10]|
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                      HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|
                      HKLM\software\microsoft\windows
 Queries value:
nt \verb|\currentversion| language pack \verb|\surrogatefallback[plane14]|
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [namespace\_callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries 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]
 Queries 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]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace]
```

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

Oueries value:

Oueries value:

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storesserviceclassinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[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\0000000000002[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]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[storesserviceclassinfo]
  Queries 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\00000000003[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\000000000003[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[enabled]
  Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \000000000004 \[version] \queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 0000000000005 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[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\00000000006[addressfamily] Oueries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 [supported name space]]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog\_entries\00000000006[storesserviceclassinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[providerinfo] Queries 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: b029-7fe99a87c641}[name] Queries value: b029-7fe99a87c641}[parentfolder] Queries value: b029-7fe99a87c641}[description] Queries value: b029-7fe99a87c641}[relativepath] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[parsingname] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[infotip] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[localizedname] Queries value: b029-7fe99a87c641}[icon] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[security] Queries value: b029-7fe99a87c641}[streamresource] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[streamresourcetype] Oueries value: b029-7fe99a87c641}[localredirectonly]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[roamable]

Oueries value:

b029-7fe99a87c641}[precreate]

Queries value:

b029-7fe99a87c641}[stream]

Oueries value:

b029-7fe99a87c641}[publishexpandedpath]

Queries value:

b029-7fe99a87c641}[attributes]

Oueries value:

b029-7fe99a87c641}[foldertypeid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[initfolderhandler]

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

folders[desktop]

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

08002b30309d}\shellfolder[attributes]

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

08002b30309d}\shellfolder[callforattributes]

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

08002b30309d}\shellfolder[restrictedattributes]

```
Queries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
 Oueries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[usedrophandler]
 Queries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
 Queries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
 Queries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
 Queries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[hideinwebview]
 Queries value:
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries 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-
 Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
 Oueries value:
08002b30309d}]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}[data]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}[generation]
                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Queries value:
409d6c4515e9}[drivemask]
                         HKLM\software\microsoft\com3[com+enabled]
 Queries value:
                         HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
 Oueries value:
 Queries value:
                         HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                         HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
 Queries value:
 Oueries value:
                         HKCR\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
                         HKLM\software\microsoft\ole[maxsxshashcount]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                         HKLM\system\currentcontrolset\services\ldap[ldapclientintegritv]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
 Queries value:
                         HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion[devicepath]
 Queries value:
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Oueries 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]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
 Queries 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]

 Queries value:
 HKCR\allfilesystemobjects[docobject]

Queries value: HKCR\allfilesystemobjects[docobj
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]

 $\label{lem:queries} Queries \ value: $$ HKCU\software\headlight\getrighttogo\sharedconfig[useloadimage] $$ HKCU\software\headlight\getrighttogo\sharedconfig[doxpthemes] $$$ 

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}\category\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a$ 

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [relative path]$ 

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'abb685 db-65 f9-4 cf6-a03a-e3 ef 65 72 9 f 3 d \ '[icon]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \folder$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \explorer \folder descriptions \folder \$ 

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \coftware \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$ 

Queries value:

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

Oueries value:

 $HKLM \coftware \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$ 

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

folders[appdata]

Queries value:

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

Oueries value:

 $HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'mountpoints2 \ 'cpc \ 'olume \ '{69d250e3-6c18-11e3-b3bc-806e6f6e6963} \ [generation]$ 

Queries 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:

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries 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:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \end{allower} In the properties of the prop$ 

Queries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[foldertypeid]

Queries value:

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

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

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus system [copyfile buffered synchronous io]$ 

 $\label{thm:continuous} Queries \ value: \\ HKCU \ software \ headlight \ getrighttogo \ shared config \ [debug]$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\[parentfolder]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[description]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ fdd 39 ad 0-238 f-46 af-46 af$ adb4-6c85480369c7}[relativepath] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[parsingname] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[infotip] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[localizedname]  $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'fdd 39 ad 0-238 f-46 af-24 af-24$ adb4-6c85480369c7}[icon] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[security] adb4-6c85480369c7}[streamresource] adb4-6c85480369c7}[streamresourcetype]  $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'fdd39ad0-238f-46af-1000' \ explorer \ 'folder descriptions' \ 'fdd39ad0-238f-46af-1000' \ explorer \ 'fdd39a$ adb4-6c85480369c7}[localredirectonly] adb4-6c85480369c7}[roamable] adb4-6c85480369c7}[precreate] adb4-6c85480369c7}[stream] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[publishexpandedpath] adb4-6c85480369c7}[attributes] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46afadb4-6c85480369c7}[foldertypeid] Oueries value:  $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ fdd 39 ad 0-238 f-46 af-46 af-46$ adb4-6c85480369c7}[initfolderhandler] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[attributes] HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[callforattributes] HKCR\clsid\{59031a47-3f72-44a7-89c5-Queries value: 5595fe6b30ee}\shellfolder[restrictedattributes] Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsfordisplay] HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[hidefolderverbs] HKCR\clsid\{59031a47-3f72-44a7-89c5-Queries value: 5595fe6b30ee}\shellfolder[usedrophandler] Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsforparsing] HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[wantsparsedisplayname] HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[queryforoverlay] HKCR\clsid\{59031a47-3f72-44a7-89c5-Queries value: 5595fe6b30ee}\shellfolder[mapnetdriveverbs] HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[queryforinfotip] HKCR\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[hideinwebview] Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[pintonamespacetree]

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

5595fe6b30ee}\shellfolder[hideondesktopperuser]

Oueries value:

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

5595fe6b30ee}\shellfolder[hasnavigationenum]

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-5595fe6b30ee}]

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

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

Queries value

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Queries value

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

Oueries value

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

Queries value:

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

Oueries 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:

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

Queries value

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

Oueries value:

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

Queries value:

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

Queries value:

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

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

folders[common desktop]

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[a58d51951bbc071eb0828eab9d9b464d]

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]