Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 40, Task ID: 157

Task ID: 157 Risk Level: 5

Date Processed: 2016-04-28 12:51:25 (UTC)

Processing Time: 61.15 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe"

Sample ID: 40
Type: basic
Owner: admin

Label: bb32f7634f66faa04bbed52fd1a61d36

Date Added: 2016-04-28 12:44:53 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gu File Size: 368296 bytes

MD5: bb32f7634f66faa04bbed52fd1a61d36

SHA256: 1afffa3ede917f9f36bde62699523e7d9a2fdd9518e16cea59a6d596ab308c4c

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: UPX

Process/Thread Events

Creates process: C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe

["C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

\Sessions\1\BaseNamedObjects\bb32f7634f66faa04bbed52fd1a61d36.exeqPZ8JcHT

Creates semaphore: \Sessions\1\BaseNamedObjects\1NI-bb32f7634f66faa04bbed52fd1a61d36.data

Creates semaphore: \Sessions\1\BaseNamedObjects\GR_FileChecker

Creates semaphore: \Sessions\1\BaseNamedObjects\GRO

Creates semaphore: \Sessions\1\BaseNamedObjects\GR_FlushingList \Creates semaphore: \Sessions\1\BaseNamedObjects\GR_Write

Creates semaphore: \Sessions\1\BaseNamedObjects\GR_GErrMsg

Creates semaphore: \Sessions\1\BaseNamedObjects\GR1
Creates semaphore: \Sessions\1\BaseNamedObjects\GR2

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

Creates semaphore: \Sessions\1\BaseNamedObjects\GR9
Creates semaphore: \Sessions\1\BaseNamedObjects\GR10
Creates semaphore: \Sessions\1\BaseNamedObjects\GR11
Creates semaphore: \Sessions\1\BaseNamedObjects\GR12

Creates semaphore: \Sessions\1\BaseNamedObjects\GR13
Creates semaphore: \Sessions\1\BaseNamedObjects\GR14
Creates semaphore: \Sessions\1\BaseNamedObjects\GR15
Creates semaphore: \Sessions\1\BaseNamedObjects\GR16
Creates semaphore: \Sessions\1\BaseNamedObjects\GR17

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

Creates semaphore: \Sessions\1\BaseNamedUbjects\GR26
Creates semaphore: \Sessions\1\BaseNamedObjects\GR27
Creates semaphore: \Sessions\1\BaseNamedObjects\GR27
Creates semaphore: \Sessions\1\BaseNamedObjects\GR28
Creates semaphore: \Sessions\1\BaseNamedObjects\GR29

Creates semaphore: \Sessions\1\BaseNamedObjects\GR30
Creates semaphore: \Sessions\1\BaseNamedObjects\GR31
Creates semaphore: \Sessions\1\BaseNamedObjects\GR31
Creates semaphore: \Sessions\1\BaseNamedObjects\GR32

Creates semaphore: \Sessions\1\BaseNamedObjects\GR32
Creates semaphore: \Sessions\1\BaseNamedObjects\GR33

\Sessions\1\BaseNamedObjects\GR34 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR35 $\verb|\Sessions|1\\BaseNamedObjects|GR36|$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR37 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR38 Creates semaphore: $\Sessions\1\BaseNamedObjects\GR39$ \Sessions\1\BaseNamedObjects\GR40 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR41 \Sessions\1\BaseNamedObjects\GR42 Creates semaphore: \Sessions\1\BaseNamedObjects\GR43 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR44 \Sessions\1\BaseNamedObjects\GR45 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR46 \Sessions\1\BaseNamedObjects\GR47 Creates semaphore: \Sessions\1\BaseNamedObjects\GR48 Creates semaphore: \Sessions\1\BaseNamedObjects\GR49 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR50 Creates semaphore: \Sessions\1\BaseNamedObjects\GR51 Creates semaphore: \Sessions\1\BaseNamedObjects\GR52 Creates semaphore: \Sessions\1\BaseNamedObjects\GR53 Creates semaphore: \Sessions\1\BaseNamedObjects\GR54 \Sessions\1\BaseNamedObjects\GR55 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR56 Creates semaphore: \Sessions\1\BaseNamedObjects\GR57 Creates semaphore: \Sessions\1\BaseNamedObjects\GR58 \Sessions\1\BaseNamedObjects\GR59 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR60 Creates semaphore: \Sessions\1\BaseNamedObjects\GR61 Creates semaphore: \Sessions\1\BaseNamedObjects\GR62 Creates semaphore: \Sessions\1\BaseNamedObjects\GR63 Creates semaphore: \Sessions\1\BaseNamedObjects\GR64 \Sessions\1\BaseNamedObjects\GR65 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR66 Creates semaphore: \Sessions\1\BaseNamedObjects\GR67 Creates semaphore: \Sessions\1\BaseNamedObjects\GR68 Creates semaphore: \Sessions\1\BaseNamedObjects\GR69 Creates semaphore: \Sessions\1\BaseNamedObjects\GR70 \Sessions\1\BaseNamedObjects\GR71 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR72 Creates semaphore: \Sessions\1\BaseNamedObjects\GR73 \Sessions\1\BaseNamedObjects\GR74 Creates semaphore: Creates semaphore: $\Sessions\1\BaseNamedObjects\GR75$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR76 \Sessions\1\BaseNamedObjects\GR77 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR78 Creates semaphore: \Sessions\1\BaseNamedObjects\GR79 \Sessions\1\BaseNamedObjects\GR80 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR81 \Sessions\1\BaseNamedObjects\GR82 Creates semaphore: \Sessions\1\BaseNamedObjects\GR83 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 Creates semaphore: \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: \Sessions\1\BaseNamedObjects\GR88 $\verb|\Sessions|1\BaseNamedObjects|| GR89$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR90 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR91 \Sessions\1\BaseNamedObjects\GR92 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR93 Creates semaphore: \Sessions\1\BaseNamedObjects\GR94 Creates semaphore: \Sessions\1\BaseNamedObjects\GR95 Creates semaphore: \Sessions\1\BaseNamedObjects\GR96 Creates semaphore: \Sessions\1\BaseNamedObjects\GR97 \Sessions\1\BaseNamedObjects\GR98 Creates semaphore: $\verb|\Sessions|1\\BaseNamedObjects|GR99|$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR100 Creates semaphore: \Sessions\1\BaseNamedObjects\INI-bb32f7634f66faa04bbed52fd1a61d36.data0

File System Events

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:

C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data0
Opens: C:\Windows\Prefetch\BB32F7634F66FAA04BBED52FD1A61-A090BD3D.pf

Opens: C:\Windows

```
C:\Windows\System32\wow64.dll
 Opens:
                         C:\Windows\SysWOW64
 Opens:
                         C:\Windows\SysWOW64\apphelp.dll
 Opens:
                         C:\Windows\Temp\bb32f7634f66faa04bbed52fd1a61d36.exe
 Opens:
 Opens:
                         C:\Windows\SysWOW64\ntdll.dll
 Opens:
                         C:\Windows\SysWOW64\kernel32.dll
                         C:\Windows\SysWOW64\KernelBase.dll
 Opens:
 Opens:
                         C:\Windows\apppatch\sysmain.sdb
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
 Opens:
                         C:\Windows\SysWOW64\oledlg.dll
 Opens:
                         C:\Windows\SysWOW64\secur32.dll
 Opens:
                         C:\Windows\SysWOW64\winspool.drv
                         C:\Windows\SysWOW64\sechost.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\combase.dll
 Opens:
                         C:\Windows\SysWOW64\SHCore.dll
 Opens:
                         C:\Windows\SysWOW64\msvcrt.dll
 Opens:
                         C:\Windows\SysWOW64\bcryptprimitives.dll
 Opens:
                         C:\Windows\SysWOW64\cryptbase.dll
 Opens:
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
                         C:\Windows\SysWOW64\user32.dll
                         C:\Windows\SysWOW64\gdi32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
                         C:\Windows\SysWOW64\comdlg32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
                         C:\Windows\SysWOW64\oleaut32.dll
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
 Opens:
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
                         C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.2.Manifest
 Opens:
 Opens:
                         C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.3.Manifest
 Opens:
                         C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.Config
 Opens:
                         C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.1000.Manifest
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local
                         C:\Windows\SysWOW64\tzres.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
                         C:\Windows\Fonts\tahoma.ttf
                         {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}
 Opens:
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
                         C:\Windows\SysWOW64\clbcatq.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\propsys.dll
                         Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x00000000000000e.db
                        C:\Users\desktop.ini
 Opens:
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin
                         C:\Users\Admin\Desktop\desktop.ini
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cfgmgr32.dll
 Opens:
                         C:\Windows\SysWOW64\devobj.dll
                         C:\Windows\SysWOW64\setupapi.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData
 Opens:
                         C:\Users\Admin\AppData\Roaming\GetRightToGo
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data
 Opens:
                         C:\Windows\Temp
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data0
 Opens:
                        C:\Windows\SysWOW64\ntmarta.dll
                         C:\Users\Admin\Desktop
 Opens:
 Opens:
                         C:\Users\Admin\Desktop\Downloads\
 Opens:
                         C:\Windows\SysWOW64\dwmapi.dll
 Opens:
                         C:\Users\Admin\Documents\desktop.ini
 Opens:
                         C:\Users\Public\desktop.ini
 Opens:
                         C:\Users\Public
 Opens:
                         C:\Users\Public\Desktop\desktop.ini
 Opens:
                         C:\Windows\Fonts\sserife.fon
 Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data
C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.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\bb32f7634f66faa04bbed52fd1a61d36.exe
```

Reads from:

C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data

Reads from:

C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data0

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

HKCU\software\headlight Creates key:

Creates key: HKCU\software\headlight\getrighttogo

HKCU\software\headlight\getrighttogo\sharedconfig Creates key: Creates key: HKCU\software\headlight\getrighttogo\customizedapps

Opens key: HKLM\software\microsoft\wow64

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

Opens key:

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

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

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

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

Opens key: HKCU\

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

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

HKCU\control panel\desktop Opens key:

HKCU\control panel\desktop\muicached Opens kev:

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

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

nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$

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

Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ nt \ current version \ limits ge \ file$

execution options

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

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions

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

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

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration

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

nt\currentversion\gre_initialize

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

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

nt\currentversion\compatibility32

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

compatibility

Opens key: HKI M\

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

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

HKLM\software\microsoft\ole Opens key:

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

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

Opens key: HKCU\software\classes\ Opens key: HKCU\software\classes\wow6432node\clsid

Opens key: HKCR\wow6432node\clsid

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

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

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\extendedlocale Opens key:

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

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

Opens key:

Opens key: HKLM\system\setup

HKLM\system\currentcontrolset\control\nls\locale Opens kev:

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

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

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

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

Opens key:

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

Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses

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

Opens key: HKLM\software\microsoft\windows

 $nt\current version\label{language} pack\datastore_v1.0$

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\37c48e35

Opens key:

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

Opens key:

Opens key

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol_catalog 9 \setminus catalog_entries$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005

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\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000001

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000000004

Opens key:

 $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| policies\\| explorer$

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\bb32f7634f66faa04bbed52fd1a61d36.exe Opens key:

 $HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\folderdescriptions| for the property of the property$

Opens key:

db2c-424c-b029-7fe99a87c641}

Opens key:

 $HKLM \label{lem:hklm} White the latest and the la$

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

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

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders$

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

folders Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key:

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta + (20d04fe0-delta + (20d0$

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum

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

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

08002b30309d}\inprocserver32

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c144, d5291c64-7c88-4c144, d5291c64-$

11e3-be65-806e6f6e6963}\

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

HKCR\drive\shellex\folderextensions Opens kev:

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\wow6432node\policies\microsoft\windows\explorer

Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer Opens key: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

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

Opens key:

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

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

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32 Opens key:

HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler32

Opens key:

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

 $\label{thm:local_hammon} \mbox{HKCU\software\mbox{\sc windows\currentversion\explorer\advanced}} \ \ \mbox{\sc windows\currentversion\explorer\advanced}} \ \mbox{\sc windows\currentversion\explorer\adv$ Opens key:

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

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

HKCR\directory Opens key:

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

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

Opens key: HKCR\folder

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

HKCR\folder\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesvstemobjects

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

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 kev: HKCR\folder\docobiect

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens key: HKCR\directory\browseinplace

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

Opens kev: HKCR\folder\browseinplace

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

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

Opens kev: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

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

HKCR\allfilesystemobjects\clsid Opens key:

Opens key: HKCU\software

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

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

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

94f2-00a0c91efb8b}

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

94f2-00a0c91efb8b}\properties

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-10explorer\} \ folder \ before \ folder \ before \ folder \ folder \ before \ folder \ fol$ 65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

Opens key:

11e3-be65-806e6f6e6963}\

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-part \ and \ barrier \ ba$ b587-4786-b4ef-bd1dc332aeae}

Opens key:

b587-4786-b4ef-bd1dc332aeae}\propertybag

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

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (fdd 39 ad 0-10 ad$ 238f-46af-adb4-6c85480369c7}

Opens kev:

238f-46af-adb4-6c85480369c7}\propertybag

HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-Opens key:

5595fe6b30ee}\shellfolder

HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-Opens key:

5595fe6b30ee}\shellfolder

 $\label{thm:local-continuous} HKCU \software \microsoft \windows \current version \explorer \clsid \clsid$ Opens key:

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

Opens key:

89c5-5595fe6b30ee}\shellfolder Opens kev:

HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\inprocserver32

HKCR\wow6432node\clsid\{4df0c730-df9d-4ae3-9153-Opens kev:

aa6b82e9795a}\inprocserver32

Opens key:

 $HKLM \label{lem:hklm} Software \label{lem:hklm} Which is the last of the las$ f20f-4863-afef-f87ef2e6ba25}

Opens key:

f20f-4863-afef-f87ef2e6ba25}\propertybag

 $HKLM \label{lem:hklm} LML \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wow 6432 node \label{lem:hklm} is consistent with lemma \label{lem:hklm} wow 6432 node \label{lem:hkklm} wow 643$ Opens kev:

shell folders

Opens key: HKLM\software\microsoft\windows $\verb|nt\currentversion\language| pack\surrogatefall back \verb|ms sans serif| \\$

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

Oueries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$ Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Oueries value:

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

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

us[alternatecodepage]

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]] \ details a software \ wow 6432 node \ microsoft \ windows \ current \ version \ side by side \ preferex \ ternal \ manifest]$

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

HKCU\software\microsoft\windows Oueries value:

nt\currentversion\appcompatflags[showdebuginfo]

Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the control of the contr$ options\dllnxoptions[usefilter]

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

```
options\dllnxoptions[bb32f7634f66faa04bbed52fd1a61d36.exe]
                         HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[bb32f7634f66faa04bbed52fd1a61d36]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
 Oueries value:
                         HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Oueries value:
                         HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Queries value:
                         HKLM\software\microsoft\ole[aggressivemtatesting]
 Oueries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
                         HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[en]
 Oueries value:
                         HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:
                         HKLM\system\setup[oobeinprogress]
 Oueries value:
                         HKLM\svstem\setup[svstemsetupinprogress]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
                         Oueries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
                         HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| ctf[enablean chorcontext]|
 Oueries value:
                         HKLM\software\microsoft\windows
 Queries 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]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane4]|
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
 Queries value:
                         HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane14]|
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus protocol\_catalog9[serial\_access\_num]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \pace_catalog 5 \catalog_entries \pace_catalog 5 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \ca$

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [version]
   Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000004[storesserviceclassinfo] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space_catalog \\ \setminus catalog_entries \setminus 00000000000004[provider info]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 0000000000005[providerid]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000005 [supported name space]]$ Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000005[storesserviceclassinfo] Queries value:

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

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 000000000006 \ [displaystring]$ Queries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le catalog \le catalog \le catalog = not in the control set \setminus services \setminus catalog \le catalo$

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

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

HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets]

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [no properties recyclebin]$

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

Queries value:

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

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4$ db2c-424c-b029-7fe99a87c641}[parsingname]

Queries value:

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

Queries value:

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

Oueries value:

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

```
db2c-424c-b029-7fe99a87c641}[security]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[streamresource]
db2c-424c-b029-7fe99a87c641}[streamresourcetype]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[localredirectonly]
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b
db2c-424c-b029-7fe99a87c641}[roamable]
    Queries value:
db2c-424c-b029-7fe99a87c641}[precreate]
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4
db2c-424c-b029-7fe99a87c641}[stream]
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4
db2c-424c-b029-7fe99a87c641}[attributes]
db2c-424c-b029-7fe99a87c641}[foldertypeid]
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
                                                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
    Queries value:
folders[desktop]
    Oueries value:
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[restrictedattributes]
    Queries value:
                                                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[foldervalueflags]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
                                                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\inprocserver32[]
    Queries value:
11e3-be65-806e6f6e6963}[data]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c
11e3-be65-806e6f6e6963}[generation]
    Queries value:
                                                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Queries value:
                                                                   HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
    Oueries value:
                                                                   HKLM\software\microsoft\com3[com+enabled]
                                                                   HKCR \\ wow 6432 \\ node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]
    Oueries value:
                                                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Queries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
    Queries value:
                                                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
                                                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
    Oueries value:
                                                                   HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:
Queries value:
                                                                   HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Oueries value:
                                                                    HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Queries 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]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
                          HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
 Queries value:
97a27216f98a}\inprocserver32[]
                          HKCR\directory[docobject]
 Queries value:
                          HKCR\folder[docobject]
 Queries value:
                          {\tt HKCR\ left} lesystemobjects [docobject]
 Oueries value:
 Queries value:
                          HKCR\directory[browseinplace]
 Queries value:
                          HKCR\folder[browseinplace]
                          HKCR\allfilesystemobjects[browseinplace]
 Queries value:
                          HKCR\directory[isshortcut]
 Queries value:
 Queries value:
                          HKCR\folder[isshortcut]
 Oueries value:
                          HKCR\allfilesystemobjects[isshortcut]
                          HKCR\directory[alwaysshowext]
 Queries value:
 Oueries value:
                          HKCR\directorv[nevershowext]
 Oueries value:
                          HKCR\folder[nevershowext]
```

Queries value: HKCR\allfilesystemobjects[nevershowext]

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

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

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

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions \cite{lem:hklmsoftware} and \cite{lem:hklmso$

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{2.0} \end{constraints} \begin{center} Albert A$

Queries value:

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

Queries value:

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

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

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

folders[appdata]

Oueries value:

 $HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'mount points 2 \ 'cpc \ 'd5291c63-7c88-11e3-be65-806e6f6e6963 \ [data]$

Queries value:

 $HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \creen{tensor} \end{tensor}$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[infotip]$

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[icon]$

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[localredirectonly]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[roamable]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]}$

Queries value:

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

Queries value:

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

Queries value:

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

b587-4786-b4ef-bd1dc332aeae}[foldertypeid]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]

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

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

Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]

HKLM\software\policies\microsoft\windows\system[copyfilechunksize] Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount] Queries value:

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

Queries value:

238f-46af-adb4-6c85480369c7}[category]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{fdd39ad0-microsoft\ windows\ current \ version\ \ \ \}$ 238f-46af-adb4-6c85480369c7}[name]

238f-46af-adb4-6c85480369c7}[parentfolder]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{fdd39ad0-microsoft\ windows\ current \ version\ \ \ \}$ 238f-46af-adb4-6c85480369c7}[description]

238f-46af-adb4-6c85480369c7}[relativepath]

238f-46af-adb4-6c85480369c7}[parsingname]

238f-46af-adb4-6c85480369c7}[infotip]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localizedname]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ descriptions \setminus \{fdd30ad0-m$ 238f-46af-adb4-6c85480369c7}[icon]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[security]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{fdd39ad0-microsoft \setminus windows \setminus current \\ descriptions \setminus \{fdd30ad0-m$ 238f-46af-adb4-6c85480369c7}[streamresource]

238f-46af-adb4-6c85480369c7}[streamresourcetype] Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (fdd 39 ad 0-10 folder \ fold$ 238f-46af-adb4-6c85480369c7}[localredirectonly]

238f-46af-adb4-6c85480369c7}[roamable] Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (fdd 39 ad 0-10 folder \ fold$ 238f-46af-adb4-6c85480369c7}[precreate]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[stream]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[publishexpandedpath]

 $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7}[attributes]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[foldertypeid]

238f-46af-adb4-6c85480369c7}[initfolderhandler]

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

folders[personal]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\shellfolder[attributes]

HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-Oueries value:

5595fe6b30ee}\shellfolder[callforattributes]

HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-Queries value:

5595fe6b30ee}\shellfolder[restrictedattributes]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c55595fe6b30ee}\shellfolder[foldervalueflags]

Queries value:

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

5595fe6b30ee}]

Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{4df0c730-df9d-4ae3-9153-

aa6b82e9795a}\inprocserver32[]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-

f20f-4863-afef-f87ef2e6ba25}[category]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [name]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}[parentfolder]

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [description]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [relative path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [parsing name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [infotip]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} \ [localized name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\}[icon]$

Queries value:

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

Queries value

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

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \mbox{$c4aa340d-f20f-4863-afef-f87ef2e6ba25}[stream resource type]$

Queries value:

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

Queries value

 $\label{thm:local-problem} HKLM \software \wow 6432 node \mbox{$c4aa340d-f20f-4863-afef-f87ef2e6ba25} [roamable]$

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*} Hklm \end{align*} Hklm \end{align*} Label{lem:hklmsoftware wow6432node \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*} Hklm \end{align*} Hklm \end{align*} Label{lem:hklmsoftware \end{align*} Hklm \end{align*$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{c4aa340d-f20f-4863-afef-f87ef2e6ba25\} [initfolder handler]$

 $Queries\ value: \ HKLM\ software\ wow 6432 node\ microsoft\ windows\ current version\ explorer\ user shell\ folders\ [common\ desktop]$

Queries value:

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

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[bb32f7634f66faa04bbed52fd1a61d36]
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]