# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 6, Task ID: 21

Task ID: 21 Risk Level: 5

Date Processed: 2016-04-28 12:46:41 (UTC)

Processing Time: 61.1 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe"

Sample ID: 6
Type: basic
Owner: admin

Label: 70c87e532c1ff4ae687b26c4224aa435

Date Added: 2016-04-28 12:44:50 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gu File Size: 368256 bytes

MD5: 70c87e532c1ff4ae687b26c4224aa435

SHA256: 28b52897659cf99851f39f4f2c0c423f55a328ba2de1f3da894a85ba624b6e9b

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\70c87e532c1ff4ae687b26c4224aa435.exe

["C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe"]

### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

\Sessions\1\BaseNamedObjects\70c87e532c1ff4ae687b26c4224aa435.exe92K4yN2z

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-70c87e532c1ff4ae687b26c4224aa435.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\T\BaseNamedObjects\GR\_GErrMsg

Creates semaphore: \Sessions\1\BaseNamedObjects\GR1 Creates semaphore: \Sessions\1\BaseNamedObjects\GR2 Creates semaphore: \Sessions\1\BaseNamedObjects\GR3 Creates semaphore: \Sessions\1\BaseNamedObjects\GR4 \Sessions\1\BaseNamedObjects\GR5 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR6 Creates semaphore: \Sessions\1\BaseNamedObjects\GR7 \Sessions\1\BaseNamedObjects\GR8 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR9 Creates semaphore: \Sessions\1\BaseNamedObjects\GR10 \Sessions\1\BaseNamedObjects\GR11 Creates semaphore: 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\GR18

Creates semaphore: \Sessions\1\BaseNamedObjects\GR20
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\BaseNamedObjects\GR26
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\GR32

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

\Sessions\1\BaseNamedObjects\GR34 Creates semaphore: \Sessions\1\BaseNamedObjects\GR35 Creates semaphore:  $\verb|\Sessions|1\\BaseNamedObjects|GR36|$ 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 Creates semaphore: \Sessions\1\BaseNamedObjects\GR71 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 Creates semaphore: \Sessions\1\BaseNamedObjects\GR92 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: Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100 Creates semaphore:  $\verb|\Sessions|1| BaseNamedObjects| INI-70c87e532c1ff4ae687b26c4224aa435.data0| \\$ 

## 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:

Opens: C:\Windows

```
C:\Windows\System32\wow64.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64
                        C:\Windows\SysWOW64\apphelp.dll
 Opens:
 Opens:
                        C:\Windows\Temp\70c87e532c1ff4ae687b26c4224aa435.exe
 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
                        C:\Windows\SysWOW64\winspool.drv
 Opens:
                        C:\Windows\SysWOW64\sechost.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\combase.dll
 Opens:
                        C:\Windows\SysWOW64\SHCore.dll
 Opens:
                        C:\Windows\SysWOW64\msvcrt.dll
                        C:\Windows\SysWOW64\bcryptprimitives.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\cryptbase.dll
                        C:\Windows\SysWOW64\sspicli.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
                        C:\Windows\SysWOW64\advapi32.dll
 Opens:
                        C:\Windows\SysWOW64\user32.dll
 Opens:
                        C:\Windows\SysWOW64\gdi32.dll
 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\70c87e532c1ff4ae687b26c4224aa435.exe.2.Manifest
 Opens:
 Opens:
                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.3.Manifest
 Opens:
                        C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.Config
 Opens:
                        C: \verb|\windows| temp| \end{|c|} 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
 Opens:
                        C:\Windows\SysWOW64\clbcatq.dll
 Opens:
                        C:\Windows\SysWOW64\propsys.dll
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
 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
 Opens:
                        C:\Windows\SysWOW64\setupapi.dll
 Opens:
                        C:\Users\Admin\AppData
 Opens:
                        C:\Users\Admin\AppData\Roaming\GetRightToGo
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data
 Opens:
                        C:\Windows\Temp
 Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0
 Opens:
                        C:\Windows\SysWOW64\ntmarta.dll
                        C:\Users\Admin\Desktop
 Opens:
 Opens:
                        C:\Users\Admin\Desktop\Downloads\
 Opens:
                        C:\Windows\SysWOW64\dwmapi.dll
                        C:\Users\Admin\Documents\desktop.ini
 Opens:
 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\70c87e532c1ff4ae687b26c4224aa435.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\70c87e532c1ff4ae687b26c4224aa435.exe
```

Reads from:

C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data

Reads from:

C:\Users\Admin\AppData\Roaming\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.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

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\software\microsoft\wow64

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

Opens key:

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

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

Opens key: HKLM\system\currentcontrol\s\customlocale
Opens key: HKLM\system\currentcontrol\s\language
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages\en-us

 $Opens\ key: \\ HKLM \ system \ current controls et \ control \ mui \ uilanguages \ pending delete$ 

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
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

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

Opens key:

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

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

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

execution options

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

options\dllnxoptions

 $Opens\;key: \\ \qquad \qquad \mathsf{HKLM} \\ system \\ \mathsf{current} \\ \mathsf{control} \\ \mathsf{lsa} \\ \mathsf{fipsalgorithmpolicy} \\$ 

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

Opens key:

 $HKLM \verb|\system| current controlset \verb|\policies| microsoft| cryptography \verb|\configuration| configuration | co$ 

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

 $\verb|nt\currentversion\gre_initialize| \\$ 

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

nt\currentversion\compatibility32

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

compatibility

Opens key: HKLM\

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

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

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

Opens key: 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
Opens key: HKLM\system\currentcontrol\set\control\nls\extendedlocale

Opens key: HKLM\software\wow6432node\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

 $Opens\;key: \\ \qquad \qquad \text{HKCU} software \verb|\microsoft| windows \verb|\currentversion| direct manipulation \\$ 

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus compatibility \setminus 70c87e532c1ff4ae687b26c4224aa435.exe$ 

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

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore\_v1.0

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows  $\verb| nt\rangle anguage| pack\surrogatefallback\ms shell dlg 2|$ 

Opens key:  $HKLM \verb|\system| current control set \verb|\services| winsock 2 \verb|\parameters| \\$ 

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\0020f864

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000005

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog\_entries$ Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000000 Opens key:

Opens key:

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

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008

Opens key: Opens key:

 $HKLM \land system \land current control set \land services \land winsock 2 \land parameters \land protocol\_catalog 9 \land catalog\_entries \land 0000000000010 \land parameters \land protocol\_catalog 9 \land catalog\_entries \land 0000000000010 \land parameters \land p$ Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000014

Opens key: 

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001

Opens key: Opens kev:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004 Opens key:

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

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

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

Opens key:

Opens key:

Opens key:

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

db2c-424c-b029-7fe99a87c641}

Opens kev:

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

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

Opens key:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ description \ for the contraction \ fo$ 

Opens key:

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

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

folders Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d808002b30309d}\shellfolder

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta \} + \{20d04f$ Opens key:

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

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

08002b30309d}\inprocserver32

Opens key:

 $\label{two-continuous} \begin{tabular}{ll} HKCU \software \mbox{$\stackrel{\cdot}{$}$ indows \current version \explorer \mbox{$\stackrel{\cdot}{$}$ mount points 2 \cpc \volume} \end{tabular}$ 

Opens key:

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: 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

HKLM\software\microsoft\com3 Opens kev:

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

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

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

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

97a27216f98a}\inprocserver32

HKCU\software\classes\directory Opens key:

HKCR\directory Opens key:

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

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

 ${\tt HKCU \backslash software \backslash classes \backslash all file system objects}$ Opens key:

Opens key: HKCR\allfilesystemobjects

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

 ${\tt HKCR\allfilesystemobjects\shellex\iconhandler}$ Opens key: Opens key: HKCU\software\classes\directory\docobject

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

HKCR\directory\browseinplace Opens kev:

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

Opens key: HKCR\folder\browseinplace

 ${\tt HKCU \ } \dot{software \ } \dot{softw$ Opens key:

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

HKCR\directory\clsid Opens kev:

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

HKCR\folder\clsid Opens key:

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

Opens key: HKCR\allfilesystemobjects\clsid

Opens key: HKCU\software

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup  $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version$ 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:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4cqc\} \ d5291c63-7c88-4cqc \ d5291c63$ 11e3-be65-806e6f6e6963}\

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

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

b587-4786-b4ef-bd1dc332aeae}

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

HKLM\software\wow6432node\policies\microsoft\windows\system

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

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

Opens key:

238f-46af-adb4-6c85480369c7}

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

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

5595fe6b30ee}\shellfolder

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

5595fe6b30ee}\shellfolder

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{59031a47-algorithms \} \setminus \{59031a47-algorit$ Opens key:

 $3f72\text{-}44a7\text{-}89c5\text{-}5595fe6b30ee} \setminus shellfolder$ 

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus (59031 \\ a47-3 \\ f72-44a7-3 \\ f$ 

89c5-5595fe6b30ee}\shellfolder

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

5595fe6b30ee}\inprocserver32

Opens key:  $HKCR\wow6432node\clsid\{4df0c730-df9d-4ae3-9153-df0d-4ae3-9150-df0d-4ae3-4df0c730-df9d-4ae3-4df0c730-df9d-4ae3-9150-df0d-4ae3-4df0c730-df9d-4ae3-4df0c730-df9d-4ae3-9150-df0d-4ae3-4df0c730-df9d-4ae3-9150-df0d-4ae3-9150-df0d-4ae3-9150-df0d-4ae3-4df0c730-df0d-4ae3-4df0c730-df0d-4ae3-4df0c730-df0d-4ae3-4$ 

aa6b82e9795a}\inprocserver32

Opens kev:

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

f20f-4863-afef-f87ef2e6ba25}

Opens kev:

f20f-4863-afef-f87ef2e6ba25}\propertybag

Opens kev:

shell folders

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

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

Queries value:

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

Oueries value:

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

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

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

us[alternatecodepage]

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

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

Queries value:

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

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

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[usefilter]

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc hilbs.} indows nt\current version\sc file execution} \\$ Oueries value:

options\dllnxoptions[70c87e532c1ff4ae687b26c4224aa435.exe]

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

 $HKLM \verb|\system| current control \verb|\sa[fipsalgorithmpolicy]|$ Oueries value:

Queries value: HKLM\software\microsoft\windows

```
nt\currentversion\gre_initialize[disablemetafiles]
                      HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\compatibilitv32[70c87e532c1ff4ae687b26c4224aa435]
 Queries value:
                       HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit dlls]
 Queries value:
                      {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap]}
 Oueries value:
                       HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                       {\tt HKLM \setminus software \setminus microsoft \setminus ole[aggressive mtatesting]}
 Oueries value:
 Oueries value:
                       HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[en]
 Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
 Oueries value:
                       HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:
                       HKLM\system\setup[oobeinprogress]
 Queries value:
                       HKLM\system\setup[systemsetupinprogress]
 Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value:
                       HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                       HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
                       HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
 Oueries value:
 Queries value:
                       HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
 Queries value:
                       HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
 Queries 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
nt\currentversion\languagepack\surrogatefallback[plane4]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
                       HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
                      HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                       HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane16]|
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
```

- 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]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[librarypath] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\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\00000000001[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\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
- 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerid]
   Queries 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]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000003 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000003 \ [provider info] \ Oueries \ value:$
- 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\00000000004[providerid]
  Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names family] \\ Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[enabled]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[version]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 000000000004 \ [storesserviceclassinfo] \ Queries \ value:$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ set alog\_entries \ (0000000000004 [provider in fo]) \ for the provider in formula and the provider i
               Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
               Queries value:
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000005 \ [displaystring]$ 

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]

Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[addressfamily]

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version] Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerinfo] Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[displaystring]

Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 000000000006 \ [address family]$ Queries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (00000000000006 \ [version]) \ and \ (version) \ and \ (ve$ Queries value:

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

 $HKLM \backslash system \backslash current control set \backslash services \backslash winsock 2 \backslash parameters [ws 2\_32 numhandle buckets]$ Queries value:

 $HKLM \verb|\software\microsoft| windows \verb|\currentversion| policies \verb|\explorer[noproperties mycomputer]|$ 

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

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

Queries value:

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

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

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

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ db2c-424c-b029-7fe99a87c641}[parsingname]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

```
db2c-424c-b029-7fe99a87c641}[streamresource]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[streamresourcetype]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[localredirectonly]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[roamable]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[precreate]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[stream]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
    Queries value:
db2c-424c-b029-7fe99a87c641}[attributes]
    Oueries value:
db2c-424c-b029-7fe99a87c641}[foldertypeid]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
    Oueries value:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[attributes]
                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[callforattributes]
                                                        Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[foldervalueflags]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
    Queries value:
                                                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[1
    Queries value:
HKCU \ software \ microsoft \ windows \ current version \ (d5291c64-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1c44-7c88-1
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, d5291c64-7c88-4cq24, d5291c64-7c86-7c88-4cq24, d5291c64-7c86-7c86-7c86-7c
11e3-be65-806e6f6e6963}[generation]
    Queries value:
                                                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
                                                        HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
    Oueries value:
a6bb2164fbd0}\inprocserver32[]
    Queries value:
                                                         HKLM\software\microsoft\com3[com+enabled]
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    Oueries value:
    Queries value:
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Oueries value:
b8dc300d9f9d}\inprocserver32[]
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Queries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
    Queries value:
                                                       HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Oueries value:
                                                        HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Queries value:
HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'advanced [showcompcolor]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
    Queries value:
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]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Queries value:

 $\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[showsuperhidden]| \\$ 

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]

Oueries value:

 $\label{thm:local_explorer} \begin{tabular}{l} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{local_explorer} advanced \cit$ 

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]

Queries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| iconsonly| \\ \end{tabular}$ 

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[showtypeoverlay]| \\$ 

Queries value:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{lem:hkcu} shows tatus bar\cite{lem:hkcu} and \cite{lem:hkcu} shows \cite{lem:hkcu$ 

Queries value: HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-

97a27216f98a}\inprocserver32[]

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

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

Queries value: HKCR\allfilesystemobjects[browseinplace]

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

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

Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value: 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:

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

Queries value:

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

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]$ 

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\ficon1

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ between the context \ folder \ between the context \ folder \ folder$ 

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{lem:hklmsoftware}\cite{lem:hklmsoftw$ 

Queries value:

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

Queries value:

 $\label{thm:local-continuous} HKLM software \noinder the wow 6432 node \\nicrosoft \\windows \\current version \\explorer \\folder descriptions \\\{1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae\}[localized name]$ 

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[icon]$$ 

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[streamresource]$ 

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae\}\[publishexpanded path]$ 

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-16b4e$ 

b587-4786-b4ef-bd1dc332aeae}[initfolderhandler] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}] Queries value: HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio] Queries value: HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension] Oueries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize] Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount] Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[debug] Oueries value:  $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7}[category] Oueries value: 238f-46af-adb4-6c85480369c7}[name] Oueries value: 238f-46af-adb4-6c85480369c7}[parentfolder] Queries value: 238f-46af-adb4-6c85480369c7}[description] Oueries value: 238f-46af-adb4-6c85480369c7}[relativepath] Queries value: 238f-46af-adb4-6c85480369c7}[parsingname] Oueries value: 238f-46af-adb4-6c85480369c7}[infotip] Queries value: 238f-46af-adb4-6c85480369c7}[localizedname] Oueries value:  $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7\[icon] Queries value: 238f-46af-adb4-6c85480369c7}[security] Oueries value:  $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7}[streamresource] Queries value: 238f-46af-adb4-6c85480369c7}[streamresourcetype] Queries value:  $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7}[localredirectonlv] Queries value: 238f-46af-adb4-6c85480369c7}[roamable] Queries value:  $HKLM \label{lem:hklm} White the latest and the la$ 238f-46af-adb4-6c85480369c7}[precreate] Queries value: 238f-46af-adb4-6c85480369c7}[stream] Oueries value: 238f-46af-adb4-6c85480369c7}[publishexpandedpath] Oueries value: 238f-46af-adb4-6c85480369c7}[attributes] Oueries value: 238f-46af-adb4-6c85480369c7}[foldertypeid] Queries value: 238f-46af-adb4-6c85480369c7}[initfolderhandler] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-Oueries value: 5595fe6b30ee}\shellfolder[attributes] HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-Queries value: 5595fe6b30ee}\shellfolder[callforattributes] Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shelfolders[personal]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[foldervalueflags]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\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:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In construction \explorer \end{array} In case \end{array} The label{lem:hklmsoftware} T$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{$c4aa340d-f20f-4863-afef-f87ef2e6ba25}[publish expanded path]$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340df20f-4863-afef-f87ef2e6ba25}[attributes]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{cases} If older two significant with the standard of the stand$ 

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\wow6432node\microsoft\windows\currentversion\explorer\user shell folders[common desktop]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[turn off spianimations]$ 

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[70c87e532c1ff4ae687b26c4224aa435]

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]