Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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 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\INI-bb32f7634f66faa04bbed52fd1a61d36.data
Creates semaphore:	\Sessions\1\BaseNamedObjects\GR_FileChecker
Creates semaphore:	\Sessions\1\BaseNamedObjects\GR0
Creates semaphore:	\Sessions\1\BaseNamedObjects\GR_FlushingList
Creates semaphore:	\Sessions\1\BaseNamedObjects\GR_Write
Creates semaphore:	\Sessions\1\BaseNamedObjects\GR_GErrMsg
Creates semaphore:	\Sessions\1\BaseNamedObjects\GR1
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\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\GR33

```
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR34
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR35
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR36
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR37
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR38
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR39
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR40
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR41
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR42
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR43
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR44
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR45
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR46
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR47
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR48
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR49
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR50
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR51
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR52
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR53
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR54
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR55
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR56
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR57
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR58
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR59
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR60
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR61
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR62
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR63
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR64
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR65
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
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR74
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR75
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR76
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR77
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR78
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR79
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR80
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR81
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR82
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR83
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
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR89
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR90
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
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR98
Creates semaphore:        \Sessions\1\BaseNamedObjects\GR99
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.data
Creates:
C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.data0
Opens:                    C:\Windows\Prefetch\BB32F7634F66FAA04BBED52FD1A61-A090BD3D.pf
Opens:                    C:\Windows
```

```
Opens:                      C:\Windows\System32\wow64.dll
Opens:                      C:\Windows\SysWOW64
Opens:                      C:\Windows\SysWOW64\apphelp.dll
Opens:                      C:\Windows\Temp\bb32f7634f66faa04bbed52fd1a61d36.exe
Opens:                      C:\Windows\SysWOW64\ntdll.dll
Opens:                      C:\Windows\SysWOW64\kernel32.dll
Opens:                      C:\Windows\SysWOW64\KernelBase.dll
Opens:                      C:\Windows\apppatch\sysmain.sdb
Opens:                      C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:                      C:\Windows\WinSxS\x86_microsoft.windows.common-
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
Opens:                      C:\Windows\SysWOW64\sechost.dll
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
Opens:                      C:\Windows\SysWOW64\gdi32.dll
Opens:                      C:\Windows\SysWOW64\shlwapi.dll
Opens:                      C:\Windows\SysWOW64\shell32.dll
Opens:                      C:\Windows\SysWOW64\comdlg32.dll
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
Opens:                      C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.2.Manifest
Opens:                      C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.3.Manifest
Opens:                      C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.Config
Opens:                      C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.1000.Manifest
Opens:                      C:\
Opens:                      C:\Users\Admin\AppData\Local
Opens:                      C:\Windows\SysWOW64\tzres.dll
Opens:                      C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens:                      C:\Windows\Fonts\tahoma.ttf
Opens:                      C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:                      C:\Windows\Fonts\StaticCache.dat
Opens:                      C:\Windows\SysWOW64\clbcatq.dll
Opens:                      C:\Windows\SysWOW64\propsys.dll
Opens:                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db
Opens:                      C:\Users\desktop.ini
Opens:                      C:\Users
Opens:                      C:\Users\Admin
Opens:                      C:\Users\Admin\Desktop\desktop.ini
Opens:                      C:\Windows\SysWOW64\cfgmgr32.dll
Opens:                      C:\Windows\SysWOW64\devobj.dll
Opens:                      C:\Windows\SysWOW64\setupapi.dll
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
Opens:                      C:\Users\Admin\Desktop
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
Writes to:
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

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\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
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
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\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions	
Opens key:	HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:	HKLM\system\currentcontrolset\control\lsa
Opens key:	
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration	
Opens key:	HKLM\software\wow6432node\microsoft\windows
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:	HKLM\
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\wow6432node\microsoft\ole
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\wow6432node\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\wow6432node\microsoft\oleaut
Opens key:	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\currentcontrolset\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:            HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key:            HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\bb32f7634f66faa04bbed52fd1a61d36.exe
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\currentversion\languagepack\datastore_v1.0
Opens key:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
Opens key:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2
Opens key:            HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key:            HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\37c48e35
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\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\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
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\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key:
HKLM\software\wow6432node\microsoft\windows\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\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
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\currentversion\explorer\sessioninfo\1\knownfolders
Opens key:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key:
```

```
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-a2d8-
08002b30309d}\shellfolder
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-
a2d8-08002b30309d}\shellfolder
  Opens key:              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
  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\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
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
  Opens key:              HKLM\software\microsoft\com3
  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}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
  Opens key:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
  Opens key:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
  Opens key:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
  Opens key:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:              HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32
  Opens key:              HKCU\software\classes\directory
  Opens key:              HKCR\directory
  Opens key:              HKCU\software\classes\directory\shellex\iconhandler
  Opens key:              HKCR\directory\shellex\iconhandler
  Opens key:              HKCU\software\classes\folder
  Opens key:              HKCR\folder
  Opens key:              HKCU\software\classes\folder\shellex\iconhandler
  Opens key:              HKCR\folder\shellex\iconhandler
  Opens key:              HKCU\software\classes\allfilesystemobjects
  Opens key:              HKCR\allfilesystemobjects
  Opens key:              HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
  Opens key:              HKCR\allfilesystemobjects\shellex\iconhandler
  Opens key:              HKCU\software\classes\directory\docobject
  Opens key:              HKCR\directory\docobject
  Opens key:              HKCU\software\classes\folder\docobject
  Opens key:              HKCR\folder\docobject
  Opens key:              HKCU\software\classes\allfilesystemobjects\docobject
  Opens key:              HKCR\allfilesystemobjects\docobject
  Opens key:              HKCU\software\classes\directory\browseinplace
  Opens key:              HKCR\directory\browseinplace
  Opens key:              HKCU\software\classes\folder\browseinplace
  Opens key:              HKCR\folder\browseinplace
  Opens key:              HKCU\software\classes\allfilesystemobjects\browseinplace
```

```
Opens key:            HKCR\allfilesystemobjects\browseinplace
Opens key:            HKCU\software\classes\directory\clsid
Opens key:            HKCR\directory\clsid
Opens key:            HKCU\software\classes\folder\clsid
Opens key:            HKCR\folder\clsid
Opens key:            HKCU\software\classes\allfilesystemobjects\clsid
Opens key:            HKCR\allfilesystemobjects\clsid
Opens key:            HKCU\software
Opens key:            HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key:            HKLM\software\microsoft\windows\currentversion\setup
Opens key:            HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:            HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}
Opens key:            HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\properties
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}\
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}\propertybag
Opens key:            HKLM\software\wow6432node\policies\microsoft\windows\system
Opens key:            HKLM\software\policies\microsoft\windows\system
Opens key:            HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}\propertybag
Opens key:            HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
Opens key:            HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
Opens key:            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}\shellfolder
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-
89c5-5595fe6b30ee}\shellfolder
Opens key:            HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\inprocserver32
Opens key:            HKCR\wow6432node\clsid\{4df0c730-df9d-4ae3-9153-
aa6b82e9795a}\inprocserver32
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}\propertybag
Opens key:            HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\user
shell folders
Opens key:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms sans serif
Queries value:        HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:        HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value:        HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value:        HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value:        HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value:        HKCU\control panel\desktop[preferreduilanguages]
Queries value:        HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value:        HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value:        HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value:        HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
Queries value:        HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\dllnxoptions[bb32f7634f66faa04bbed52fd1a61d36.exe]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries 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]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries 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]
  Queries 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]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  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]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:              HKLM\software\microsoft\windows
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]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
```

```
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
     Queries 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]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
     Queries 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]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
     Queries 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\000000000004[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
     Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[icon]
    Queries value:
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
    Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
    Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
    Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
    Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[foldervalueflags]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
    Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
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[]
    Queries value: HKLM\software\microsoft\com3[com+enabled]
    Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
    Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
    Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[]
    Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
    Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Queries value:

```
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
    Queries 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]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
    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\headlight\getrighttogo\sharedconfig[doxpthemes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
    Queries value:
HKLM\software\wow6432node\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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
    Queries value:
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-11e3-be65-806e6f6e6963}[generation]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[attributes]
    Queries value:

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]
    Queries value:                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]
    Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
    Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
    Queries 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]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[precreate]
    Queries value:
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]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
238f-46af-adb4-6c85480369c7}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-
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]
    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:
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]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[initfolderhandler]
    Queries value:                HKLM\software\wow6432node\microsoft\windows\currentversion\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]
```