# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 9, Task ID: 36

Task ID: 36 Risk Level:

Date Processed: 2016-04-28 12:46:55 (UTC)

Processing Time: 63.0 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe"

Sample ID: 9 Type: basic admin Owner:

83323edb74ebd75cdc7ef98e3daddd07 Label:

Date Added: 2016-04-28 12:44:50 (UTC)

PE32:win32:gui File Type: File Size: 368272 bytes

83323edb74ebd75cdc7ef98e3daddd07 MD5:

c56d96269d96d7a66021934c404ec40b89008c51c80760a96c6b25ce307b3183 SHA256:

Description: None

### Pattern Matching Results

2 PE: Nonstandard section

5 Packer: UPX

5 PE: Contains compressed section

#### Static Events

Anomaly: PE: Contains a virtual section

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

Packer:

#### Process/Thread Events

Creates process: C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe

["C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe"]

### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

\Sessions\1\BaseNamedObjects\83323edb74ebd75cdc7ef98e3daddd07.exeDjCLPpmt

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

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

Creates event: \KernelObjects\MaximumCommitCondition

Creates semaphore:  $\verb|\Sessions| 1 \\ BaseNamedObjects \\ INI-83323edb74ebd75cdc7ef98e3daddd07.data \\ Abstraction of the control of$ 

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

Creates semaphore: \Sessions\1\BaseNamedObjects\GR0

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

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

Creates semaphore: \Sessions\1\BaseNamedObjects\GR11 Creates semaphore: \Sessions\1\BaseNamedObjects\GR12  $\verb|\Sessions|1| BaseNamedObjects| GR13|$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR14 Creates semaphore: \Sessions\1\BaseNamedObjects\GR15 \Sessions\1\BaseNamedObjects\GR16 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR17 \Sessions\1\BaseNamedObjects\GR18 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR19 \Sessions\1\BaseNamedObjects\GR20 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR21

Creates semaphore: \Sessions\1\BaseNamedObjects\GR22 Creates semaphore: \Sessions\1\BaseNamedObjects\GR23 Creates semaphore: \Sessions\1\BaseNamedObjects\GR24 Creates semaphore: \Sessions\1\BaseNamedObjects\GR25 \Sessions\1\BaseNamedObjects\GR26 Creates semaphore:

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

\Sessions\1\BaseNamedObjects\GR30 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR31 Creates semaphore: \Sessions\1\BaseNamedObjects\GR32 \Sessions\1\BaseNamedObjects\GR33 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR34 Creates semaphore: \Sessions\1\BaseNamedObjects\GR36 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR37 Creates semaphore: \Sessions\1\BaseNamedObjects\GR38 Creates semaphore: \Sessions\1\BaseNamedObjects\GR39 \Sessions\1\BaseNamedObjects\GR40 Creates semaphore: Creates semaphore:  $\Sessions\1\BaseNamedObjects\GR41$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR42 \Sessions\1\BaseNamedObjects\GR43 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR44 Creates semaphore: \Sessions\1\BaseNamedObjects\GR45 \Sessions\1\BaseNamedObjects\GR46 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR47 Creates semaphore: \Sessions\1\BaseNamedObjects\GR48 Creates semaphore: \Sessions\1\BaseNamedObjects\GR49 Creates semaphore: \Sessions\1\BaseNamedObjects\GR50 Creates semaphore: \Sessions\1\BaseNamedObjects\GR51 \Sessions\1\BaseNamedObjects\GR52 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR53 Creates semaphore: \Sessions\1\BaseNamedObjects\GR54 Creates semaphore: \Sessions\1\BaseNamedObjects\GR55 Creates semaphore: \Sessions\1\BaseNamedObjects\GR56 Creates semaphore: \Sessions\1\BaseNamedObjects\GR57 Creates semaphore: \Sessions\1\BaseNamedObjects\GR58 Creates semaphore: \Sessions\1\BaseNamedObjects\GR59 Creates semaphore: \Sessions\1\BaseNamedObjects\GR60 \Sessions\1\BaseNamedObjects\GR61 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR62 Creates semaphore: \Sessions\1\BaseNamedObjects\GR63 \Sessions\1\BaseNamedObjects\GR64 Creates semaphore: Creates semaphore:  $\Sessions\1\BaseNamedObjects\GR65$ \Sessions\1\BaseNamedObjects\GR66 Creates semaphore: \Sessions\1\BaseNamedObjects\GR67 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR68 Creates semaphore: \Sessions\1\BaseNamedObjects\GR69 \Sessions\1\BaseNamedObjects\GR70 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR71 \Sessions\1\BaseNamedObjects\GR72 Creates semaphore: \Sessions\1\BaseNamedObjects\GR73 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR74 \Sessions\1\BaseNamedObjects\GR75 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR76 Creates semaphore: \Sessions\1\BaseNamedObjects\GR77 Creates semaphore: \Sessions\1\BaseNamedObjects\GR78 Creates semaphore: \Sessions\1\BaseNamedObjects\GR79 \Sessions\1\BaseNamedObjects\GR80 Creates semaphore: \Sessions\1\BaseNamedObjects\GR81 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR82 \Sessions\1\BaseNamedObjects\GR83 Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR88 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 \Sessions\1\BaseNamedObjects\GR94 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR95 Creates semaphore: \Sessions\1\BaseNamedObjects\GR96 Creates semaphore: \Sessions\1\BaseNamedObjects\GR97 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-83323edb74ebd75cdc7ef98e3daddd07.data0

## File System Events

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

Creates: C:\Users\Admin\AppData

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

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

Creates:

```
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data0
                                                      C:\Windows\Prefetch\83323EDB74EBD75CDC7EF98E3DADD-D736B47D.pf
   Opens:
   Opens:
                                                      C:\Windows
   Opens:
                                                      C:\Windows\System32\wow64.dll
                                                      C:\Windows\System32\wow64win.dll
   Opens:
   Opens:
                                                      C:\Windows\System32\wow64cpu.dll
   Opens:
                                                      C:\Windows\system32\wow64log.dll
   Opens:
                                                      C:\Windows\SysWOW64
   Opens:
                                                      C:\Windows\SysWOW64\sechost.dll
   Opens:
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.Local\
   Opens:
                                                      C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                                                      C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
   Opens:
                                                      C:\windows\temp\oledlg.dll
   Opens:
                                                      C:\Windows\SysWOW64\oledlg.dll
   Opens:
                                                      C:\windows\temp\Secur32.dll
   Opens:
                                                      C:\Windows\SysWOW64\secur32.dll
   Opens:
                                                      C:\windows\temp\WINSPOOL.DRV
   Opens:
                                                      C:\Windows\SysWOW64\winspool.drv
                                                      C:\Windows\SysWOW64\imm32.dll
   Opens:
   Opens:
                                                      C:\Windows\WindowsShell.Manifest
   Opens:
                                                      C:\Windows\SysWOW64\uxtheme.dll
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.2.Manifest
   Opens:
   Opens:
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.3.Manifest
   Opens:
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.Config
   Opens:
                                                      C: \verb|\windows\Temp\83323edb74ebd75cdc7ef98e3daddd07.exe|
   Opens:
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07.exe.1000.Manifest
   Opens:
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07ENU.dll
   Opens:
                                                      C:\windows\temp\83323edb74ebd75cdc7ef98e3daddd07L0C.dll
   Opens:
   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\temp\dwmapi.dll
   Opens:
                                                      C:\Windows\SysWOW64\dwmapi.dll
   Opens:
                                                      C:\Windows\Globalization\Sorting\SortDefault.nls
                                                      C:\Windows\SysWOW64\ole32.dll
   Opens:
   Opens:
                                                      C:\Windows\SysWOW64\rpcss.dll
   Opens:
                                                      C:\Windows\Fonts\StaticCache.dat
   Opens:
                                                      C:\Windows\SysWOW64\shell32.dll
   Opens:
                                                      C:\Users\Admin\Desktop
   Opens:
                                                      C:\Windows\SysWOW64\propsys.dll
   Opens:
                                                      \label{lem:c:start} C: \Users \land Admin \land App Data \land Local \land Microsoft \land Windows \land Caches \land cversions. 1. db
   Opens:
                                                      C:\windows\temp\ntmarta.dll
                                                      C:\Windows\SysWOW64\ntmarta.dll
   Opens:
   Opens:
                                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
                                                      C:\Users\desktop.ini
   Opens:
                                                      C:\Users
   Opens:
   Opens:
                                                      C:\Users\Admin
   Opens:
                                                      C:\Users\Admin\Desktop\desktop.ini
                                                      C:\Windows\SysWOW64\en-US\setupapi.dll.mui
   Opens:
                                                      C:\Users\Admin\AppData\Roaming
   Opens:
                                                      C:\Users\Admin\AppData
   Opens:
                                                      C:\Users\Admin\AppData\Roaming\GetRightToGo
   Opens:
   Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data
   Opens:
                                                      C:\Windows\Temp
   Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data0
   Opens:
                                                      C:\Users\Admin\Desktop\Downloads\
   Opens:
                                                      C:\Users\Admin\Documents
   Opens:
                                                      C:\Users\Admin\Documents\desktop.ini
                                                      C:\Users\Public\Desktop
   Opens:
   Opens:
                                                      C:\Users\Public\desktop.ini
                                                      C:\Users\Public
   Opens:
                                                      C:\Users\Public\Desktop\desktop.ini
   Opens:
   Opens:
                                                      C:\Windows\Fonts\sserife.fon
   Writes to:
C:\Users\Admin\AppData\Roaming\GetRightToGo\83323edb74ebd75cdc7ef98e3daddd07.data
C: \verb|Vsers| Admin| AppData| Roaming \\ GetRightToGo| 83323edb74ebd75cdc7ef98e3daddd07.data0| AppData| AppData|
   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\83323edb74ebd75cdc7ef98e3daddd07.exe
C: \verb|Vusers| Admin| AppData| Roaming | GetRightToGo| 83323edb74ebd75cdc7ef98e3daddd07.data| AppData| AppData|
```

Reads from:

 $C: \verb|Vsers| Admin| AppData| Roaming | GetRightToGo| 83323edb74ebd75cdc7ef98e3daddd07.data0| GetRightToGo| GetRig$ 

C:\Users\Admin\Documents\desktop.ini Reads from: 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\windows nt\currentversion\image file execution

options

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

HKLM\software\microsoft\wow64 Opens key:

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

execution options

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

Opens key:

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

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

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

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

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

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

Opens key: HKCU\

 $\label{thm:local_machine} \begin{tabular}{ll} HKCU\control panel\desktop\muicached\machinelanguageconfiguration \\ \end{tabular}$ Opens key: Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens kev:  ${\it HKCU} \ control\ panel\ desktop\ language configuration$ 

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside Opens kev:

Opens key:

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

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

Opens key: HKI M\

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

nt\currentversion\diagnostics

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

nt\currentversion\gre\_initialize

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

nt\currentversion\compatibility32

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

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

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

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:  $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt microsoft\windows\currentversion\spaceshape}} \mbox{\tt policies\explorer} \mbox{\tt explorer} \mbox{\tt$ Opens key: HKCU\software\microsoft\windows\currentversion\policies\network Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32

HKLM\system\currentcontrolset\control\nls\extendedlocale Opens kev: Opens key: HKLM\system\currentcontrolset\control\cmf\config

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ 83323 edb 74 ebd 75 cdc 7ef 98e 3 daddd 07. execond \ microsoft \ microsoft \ make \ microsoft \ make \ microsoft \$ Opens key:

 $0 fb 58b 01c 4a4 \} \\ language profile \\ 0x 000 000 000 \\ \{0001 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 0x 000 000 000 \\ 10x 000 000$  $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b$ Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

 $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| ctf \verb|\software\\|$ Opens key:

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 kev:

nt\currentversion\languagepack\surrogatefallback HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Opens key: HKLM\software\policies\microsoft\sqmclient\windows HKLM\software\microsoft\sqmclient\windows Opens key: Opens key:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\2cdb6258 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: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008 Opens key: Opens key:  $HKLM \land system \land current control set \land services \land winsock 2 \land parameters \land protocol\_catalog9 \land catalog\_entries \land 000000000010 \land parameters \land protocol\_catalog9 \land catalog\_entries \land 0000000000010 \land parameters \land para$ HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000028 Opens key: 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\000000000000 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 kev: 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 kev: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions Opens key: db2c-424c-b029-7fe99a87c641} Opens kev: db2c-424c-b029-7fe99a87c641}\propertybag HKCU\software\microsoft\windows\currentversion\explorer Opens key: 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 kev: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder$ 

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

 $HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + (20d04feo-block) +$ 

Opens key:

Opens key:

Opens key:

08002b30309d}\shellfolder

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 kev:

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

Opens kev:

11e3-a68e-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

Opens key:  $HKCU \setminus software \land classes \land drive \land shellex \land folder extensions \land \{fbeb8a05-beee-beed extensions \land \{fbeb8a05-beed extensions \} \}$ 

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

Opens key: HKLM\software\microsoft\com3

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas Opens key:

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

 $HKCR \setminus wow6432 node \\ clsid \\ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\} \\ \\ \\ treatas$ 

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

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

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

Opens key: HKLM\system\currentcontrolset\services\ldap

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

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ shell registered applications \ urlassociations \ directory \ open with progids$ 

Opens key:

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

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directorv

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

Opens key: HKCR\directory\curver 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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens kev: HKCR\directory\browseinplace

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 Opens key: HKCR\folder\clsid

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

Opens key: HKCR\allfilesystemobjects\clsid

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\software\wow6432node\microsoft\rpc

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key:

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

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens kev:

11e3-a68e-806e6f6e6963}\

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

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

 $Opens \; key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ language pack \ surrogate fall back \ segoe \; ui \\$ 

Opens key

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)$ 

Opens kev:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-

 $238f-46af-adb4-6c85480369c7 \} \verb|\property| bag$ 

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

5595fe6b30ee}\shellfolder

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

5595fe6b30ee}\shellfolder

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

Opens key

89c5-5595fe6b30ee}\shellfolder

Opens key:

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

Opens key:

 $\label{local-equ$ 

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\software\microsoft\windows nt\currentversion\image file execution

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Queries value:

 $\label{lem:hamman} HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] \\ Queries\ value: HKLM\system\currentcontrolset\control\nls\customlocale[empty] \\$ 

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:

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

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

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

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[83323edb74ebd75cdc7ef98e3daddd07] 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\system\currentcontrolset\control\nls\customlocale[en-us]

```
Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:
                                    HKLM\system\currentcontrolset\control\cmf\config[system]
  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]
                                    HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
                                    HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
                                    HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:
  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]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                                    HKLM\software\microsoft\windows
  Queries value:
\verb|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]
                                    HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
  Queries value:
                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane15]|
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                                    HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000003 \ [packed catalog item]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Oueries 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\00000000007[packedcatalogitem]
```

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

Queries value:

Oueries value:

Queries 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\00000000001[librarypath]
   Oueries 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]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring]
  Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog \catalog\_entries \namespace\_catalog \catalog\_entries \catalog \catalog\_entries \catalog \catalog\_entries \catalog \cat$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[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\000000000003[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 000000000003 \ [storesservice class info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
- $\label{lem:hklm} \begin{tabular}{ll} HKLM\system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catalog 5 \catalog\_entries \namespace] \end{tabular} \begin{tabular}{ll} Queries value: \namespace\_catalog 5 \catalog\_entries \namespace\_catalog$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[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\00000000005[providerid]
  Oueries value:

Oueries value:

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

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

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

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

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

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

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

Queries value.

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

Queries value:

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

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

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

 $\label{thm:microsoftwindows} HKLM software \noindows \$ 

Queries value:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gamm$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma[]{\colorer.pdf} \end{subarrange} held the subarrange of the s$ 

Queries value:

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

Oueries value:

 $\label{local-control} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder\$ 

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

Queries value:

 $\label{local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gamm$ 

Queries 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]
   Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b
db2c-424c-b029-7fe99a87c641}[attributes]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[foldertypeid]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[initfolderhandler]
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[desktop]
   Queries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[callforattributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                            Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[quervforinfotip]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
   Queries value:
                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
   Queries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
  Queries value:
HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mount points 2 \ cpc \ volume \ \{8063a3d4-8213-42444, and \ before \
11e3-a68e-806e6f6e6963}[data]
   Oueries value:
11e3-a68e-806e6f6e6963}[generation]
                                             HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Queries value:
409d6c4515e9}[drivemask]
   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[]
   Queries value:
                                            HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
   Queries value:
                                            HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
HKLM \verb|\system| current control \verb|\sa| access providers [marta extension]|
   Oueries value:
                                            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
                                             HKLM \setminus system \setminus current control set \setminus services \setminus ldap [use old host resolution order]
   Oueries value:
                                             HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
```

```
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
                       HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Oueries value:
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
```

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

Queries value:

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

Oueries value:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced[hideicons]}}$ 

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

Queries value:

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

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

Oueries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]$ 

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} and \cite{tabular} is a constant \cite{tabular} is a constant \cite{tabular} and \$ 

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

Oueries value: HKCR\allfilesvstemobiects[docobiect] Queries value: HKCR\directory[browseinplace] HKCR\folder[browseinplace] Oueries value:

HKCR\allfilesystemobjects[browseinplace] Queries value:

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

HKCR\allfilesystemobjects[isshortcut] Oueries value:

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

Queries value: HKCR\allfilesystemobjects[nevershowext]

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

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

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Oueries value

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

Queries 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

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

Oueries value

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

Queries value

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

Queries value:

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

folders[appdata]

Queries value:

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

Queries value:

 $\label{local-hamman} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae \cite{local-hamman} [name]$ 

Queries value:

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

Queries value:

 $\label{local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fill\\ b587-4786-b4ef-bd1dc332aeae\fill\\ [description]$ 

Queries value:

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]$ 

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Queries value:

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

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

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

Queries value:

 $\label{lem:hkcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \ [data]$ 

Queries value:

 $HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \cite{Microsoft} \end{substitute}$ 

Oueries value:

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

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:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\[category\]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [name]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [parent folder]$ 

Oueries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(description)\f(desc$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(relative path)\f(relative path)\f(relative$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\cite{Abstraction}\cite{Abst$ 

Queries value:

 $\label{limit} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[infotip]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\} [localized name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(icon)\f(icon)\f$ 

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\[security]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[streamresource]$ 

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[streamresourcetype]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\} [local redirectonly]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\f(roamable)\f(roamabl$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\fdd39ad0-238f-46af-adb4-6c85480369c7\}[precreate]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{fdd 39ad 0-238f-46af-adb 4-6c85480369c7\}[stream]$ 

Oueries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[publishexpandedpath]$ 

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(fdd39ad0-238f-46af-adb4-6c85480369c7)\[attributes\]$ 

Queries value:

 $HKLM\ software \ wow 6432 node \ icrosoft\ windows \ current version \ explorer\ folder descriptions \ \{fdd39ad0-fdd39$ 

```
238f-46af-adb4-6c85480369c7}[foldertypeid]
   Oueries value:
238f-46af-adb4-6c85480369c7}[initfolderhandler]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
   Queries value:
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[attributes]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[callforattributes]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[restrictedattributes]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[wantsfordisplay]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[hidefolderverbs]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[usedrophandler]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[wantsforparsing]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[wantsparsedisplayname]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[queryforoverlay]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[mapnetdriveverbs]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[queryforinfotip]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[hideinwebview]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[hideondesktopperuser]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[wantsaliasednotifications]
   Oueries value:
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Oueries value:
5595fe6b30ee}\shellfolder[nofilefolderjunction]
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
   Queries value:
5595fe6b30ee}\shellfolder[pintonamespacetree]
   Queries value:
                                             HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-
5595fe6b30ee}1
   Queries value:
f20f-4863-afef-f87ef2e6ba25}[category]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[name]
   Oueries value:
f20f-4863-afef-f87ef2e6ba25}[parentfolder]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[description]
   Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{c4aa340d-microsoft\ windows\ current \ version\ \ \}
f20f-4863-afef-f87ef2e6ba25}[relativepath]
   Queries value:
HKLM \label{lem:hklm} White the software \label{lem:hkklm} White the software \label{lem:hkk
f20f-4863-afef-f87ef2e6ba25}[parsingname]
   Oueries value:
f20f-4863-afef-f87ef2e6ba25}[infotip]
   Queries value:
HKLM \label{lem:hklm} White the software \label{lem:hkklm} White the software \label{lem:hkk
f20f-4863-afef-f87ef2e6ba25}[localizedname]
   Oueries value:
f20f-4863-afef-f87ef2e6ba25}[icon]
   Oueries value:
f20f-4863-afef-f87ef2e6ba25}[security]
   Oueries value:
f20f-4863-afef-f87ef2e6ba25}[streamresource]
   Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-
f20f-4863-afef-f87ef2e6ba25}[streamresourcetype]
   Oueries value:
```

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{c4aa340d-microsoft\ windows\ current \ version\ \ \}$ 

f20f-4863-afef-f87ef2e6ba25}[localredirectonly]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:  $HKLM\software\wow6432$ node\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[83323edb74ebd75cdc7ef98e3daddd07]

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]