# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 40, Task ID: 160

Task ID: 160 Risk Level:

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

Processing Time: 61.14 seconds Virtual Environment: IntelliVM

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

Sample ID: Type: basic admin Owner:

bb32f7634f66faa04bbed52fd1a61d36 Label:

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

File Type: File Size: 368296 bytes

bb32f7634f66faa04bbed52fd1a61d36 MD5:

1afffa3ede917f9f36bde62699523e7d9a2fdd9518e16cea59a6d596ab308c4c 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\bb32f7634f66faa04bbed52fd1a61d36.exe

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

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:

Creates semaphore:

Creates semaphore: Creates semaphore:

Creates semaphore:

\Sessions\1\BaseNamedObjects\bb32f7634f66faa04bbed52fd1a61d36.exeI97xo5zC

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:  $\verb|\Sessions| 1 \\ BaseNamedObjects \\ INI-bb32f7634f66faaO4bbed52fd1a61d36.data \\ Abstraction of the control of$ 

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 \Sessions\1\BaseNamedObjects\GR13 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR14 Creates semaphore: \Sessions\1\BaseNamedObjects\GR15 Creates semaphore: \Sessions\1\BaseNamedObjects\GR16 Creates semaphore: \Sessions\1\BaseNamedObjects\GR17 \Sessions\1\BaseNamedObjects\GR18 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR19 \Sessions\1\BaseNamedObjects\GR20 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR21 Creates semaphore: \Sessions\1\BaseNamedObjects\GR22 Creates semaphore: \Sessions\1\BaseNamedObjects\GR23 Creates semaphore: \Sessions\1\BaseNamedObjects\GR24 Creates semaphore: \Sessions\1\BaseNamedObjects\GR25

\Sessions\1\BaseNamedObjects\GR26

\Sessions\1\BaseNamedObjects\GR27

\Sessions\1\BaseNamedObjects\GR28

\Sessions\1\BaseNamedObjects\GR29

\Sessions\1\BaseNamedObjects\GR30 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR31 \Sessions\1\BaseNamedObjects\GR32 Creates semaphore: \Sessions\1\BaseNamedObjects\GR33 Creates semaphore: \Sessions\1\BaseNamedObjects\GR34 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR36 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR37 Creates semaphore: \Sessions\1\BaseNamedObjects\GR38 Creates semaphore: \Sessions\1\BaseNamedObjects\GR39 \Sessions\1\BaseNamedObjects\GR40 Creates semaphore: Creates semaphore:  $\Sessions\1\BaseNamedObjects\GR41$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR42 \Sessions\1\BaseNamedObjects\GR43 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR44 Creates semaphore: \Sessions\1\BaseNamedObjects\GR45 \Sessions\1\BaseNamedObjects\GR46 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR47 Creates semaphore: \Sessions\1\BaseNamedObjects\GR48 Creates semaphore: \Sessions\1\BaseNamedObjects\GR49 Creates semaphore: \Sessions\1\BaseNamedObjects\GR50 Creates semaphore: \Sessions\1\BaseNamedObjects\GR51 \Sessions\1\BaseNamedObjects\GR52 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR53 Creates semaphore: \Sessions\1\BaseNamedObjects\GR54 Creates semaphore: \Sessions\1\BaseNamedObjects\GR55 Creates semaphore: \Sessions\1\BaseNamedObjects\GR56 Creates semaphore: \Sessions\1\BaseNamedObjects\GR57 Creates semaphore: \Sessions\1\BaseNamedObjects\GR58 Creates semaphore: \Sessions\1\BaseNamedObjects\GR59 Creates semaphore: \Sessions\1\BaseNamedObjects\GR60 \Sessions\1\BaseNamedObjects\GR61 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR62 Creates semaphore: \Sessions\1\BaseNamedObjects\GR63 \Sessions\1\BaseNamedObjects\GR64 Creates semaphore: Creates semaphore:  $\Sessions\1\BaseNamedObjects\GR65$ \Sessions\1\BaseNamedObjects\GR66 Creates semaphore: \Sessions\1\BaseNamedObjects\GR67 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR68 Creates semaphore: \Sessions\1\BaseNamedObjects\GR69 \Sessions\1\BaseNamedObjects\GR70 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR71 \Sessions\1\BaseNamedObjects\GR72 Creates semaphore: \Sessions\1\BaseNamedObjects\GR73 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR74 \Sessions\1\BaseNamedObjects\GR75 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR76 Creates semaphore: \Sessions\1\BaseNamedObjects\GR77 Creates semaphore: \Sessions\1\BaseNamedObjects\GR78 Creates semaphore: \Sessions\1\BaseNamedObjects\GR79 \Sessions\1\BaseNamedObjects\GR80 Creates semaphore: \Sessions\1\BaseNamedObjects\GR81 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR82 \Sessions\1\BaseNamedObjects\GR83 Creates semaphore: \Sessions\1\BaseNamedObjects\GR84 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR85 \Sessions\1\BaseNamedObjects\GR86 Creates semaphore: \Sessions\1\BaseNamedObjects\GR87 Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR88  $\verb|\Sessions|1\\BaseNamedObjects|GR89|$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR90 Creates semaphore: \Sessions\1\BaseNamedObjects\GR91 Creates semaphore: \Sessions\1\BaseNamedObjects\GR92 Creates semaphore: \Sessions\1\BaseNamedObjects\GR93 \Sessions\1\BaseNamedObjects\GR94 Creates semaphore:  $\verb|\Sessions|1\BaseNamedObjects|| GR95||$ Creates semaphore: Creates semaphore: \Sessions\1\BaseNamedObjects\GR96 Creates semaphore: \Sessions\1\BaseNamedObjects\GR97 Creates semaphore:  $\verb|\Sessions|1\BaseNamedObjects|| GR98||$ Creates semaphore: \Sessions\1\BaseNamedObjects\GR99 Creates semaphore: \Sessions\1\BaseNamedObjects\GR100

Creates semaphore: \Sessions\1\BaseNamedObjects\INI-bb32f7634f66faa04bbed52fd1a61d36.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

 $\label{lem:condition} Creates: $C:\Users\land Admin\AppData\Roaming\GetRightToGo. $C:\Users\land Admin\AppData\Roaming\GetRightToGo. $$C:\Users\land Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\GetRightToGo. $$C:\Users\Admin\AppData\Roaming\App$ 

Creates:

```
Creates
C: \verb|Vsers| Admin| AppData| Roaming \\ GetRightToGo\\ bb32f7634f66faa04bbed52fd1a61d36.data0\\
                                                             C:\Windows\Prefetch\BB32F7634F66FAA04BBED52FD1A61-A090BD3D.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\bb32f7634f66faa04bbed52fd1a61d36.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-
    Opens:
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\bb32f7634f66faa04bbed52fd1a61d36.exe.2.Manifest
    Opens:
    Opens:
                                                             C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.3.Manifest
    Opens:
                                                             C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.Config
    Opens:
                                                             C:\Windows\Temp\bb32f7634f66faa04bbed52fd1a61d36.exe
    Opens:
                                                             C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36.exe.1000.Manifest
    Opens:
                                                             C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36ENU.dll
    Opens:
                                                             C:\windows\temp\bb32f7634f66faa04bbed52fd1a61d36L0C.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{local-Microsoft-Windows-Caches-Constant} C: \Users \land Admin \land App Data \land Local \land Microsoft \land Windows \land Caches \land 
    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
    Opens:
                                                            C:\Users\desktop.ini
    Opens:
                                                            C:\Windows\SysWOW64\en-US\setupapi.dll.mui
    Opens:
    Opens:
                                                            C:\Users\Admin
                                                             C:\Users\Admin\Desktop\desktop.ini
    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\bb32f7634f66faa04bbed52fd1a61d36.data
    Opens:
                                                             C:\Windows\Temp
    Opens:
C:\Users\Admin\AppData\Roaming\GetRightToGo\bb32f7634f66faa04bbed52fd1a61d36.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\bb32f7634f66faa04bbed52fd1a61d36.data
C: \verb|Vsers| 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
                                                             C:\Windows\Temp\bb32f7634f66faa04bbed52fd1a61d36.exe
    Reads from:
C: \verb|Vusers| Admin| AppData| Roaming | GetRightToGo| bb32f7634f66faa04bbed52fd1a61d36.data| data | GetRightToGo| bb32f7634f66faa04bbdd52fd1a61d36.data| data | GetRightToGo| bb32f7634f66faa04bbdd52ff66faa04bbdd52ff66faa04bbdd52ff66faa04bbdd52ff66faa04bbdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff6faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa04bdd52ff66faa
```

Reads from:

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

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

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 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:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer \end{tabular}$ 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:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ bb 32f7634f66faa 04bbed 52fd1a 61d36.exe$  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 -$ Opens key:

 $0 fb 58b 01c 4a4 \} \\ language profile \\ 0x 000 000 000 \\ \{0001 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 0x 000 000 000 \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a ea e 25577436\} \\ language profile \\ 100 1 bea 3-ed 56-483 d-a 2e 2-a e 265764 d-a 2e 2-a e 26576 d-a 2e 2-a e 2657$  $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b$ Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

 $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| ctf \verb|\software\\| wow 6432 node \verb|\microsoft\\| ctf \verb|\software\\| wow 6432 node \verb|\microsoft\\| ctf \verb|\software\\| ctf \>| ctf$ 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\37c48e35 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000005 Opens key:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog\_entries$ 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 key: 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 Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

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

08002b30309d}\shellfolder

a2d8-08002b30309d}\shellfolder

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

Opens key:

Opens key:

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:  $HKCU \setminus software \land classes \land drive \land shell ex \land folder extensions \land \{fbeb8a05-beee-beed extensions \land \{fbeb8a05-beed extensions \} \}$ 

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\wow6432node\microsoft\windows\currentversion

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

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

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

Opens key: HKCU\software

Opens key:

11e3-a68e-806e6f6e6963}\

Opens key:

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

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:

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\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens kev:

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

238f-46af-adb4-6c85480369c7}

Opens key:

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

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

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:

89c5-5595fe6b30ee}\shellfolder

Opens key:

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

Opens key:

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\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:

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

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

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

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\system\currentcontrolset\control\nls\customlocale[en-us]Queries value:HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

```
Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\customlocale[en]
                                   HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                   HKLM\svstem\setup[oobeinprogress]
  Oueries value:
  Oueries value:
                                   HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                   HKLM\system\currentcontrolset\control\nls\language groups[1]
  Oueries value:
  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 \verb|\software\\| wow 6432 node\\| microsoft\\| ctf[enable anchor context]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                                   HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane1]|
                                   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                                  HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                                   HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane4]|
                                   HKLM\software\microsoft\windows
  Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane5]|
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
                                   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                                   HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
  Oueries value:
                                   HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries 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]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
  Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000007 \ [packed catalog item]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [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\00000000001[enabled]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring] 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\0000000000002[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\0000000000002[storesserviceclassinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo] 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]
  Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000000004 \ [displaystring] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[addressfamily]
   Oueries 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]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]
   Oueries value:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005[supported name space]]
       Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled]
       Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ (version) \ and \ services \ (version) \ and \ (
       Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo]
       Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
       Queries value:
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog5 \ (catalog\_entries \ 000000000006 [library path])$ Queries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000006[providerid]$ Queries value:

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

Queries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (0000000000006 \ [version]) \ details \$ 

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets]

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

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

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

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

Queries value:

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

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[category]

Oueries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[parentfolder]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[description] Queries value:

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

Oueries value:

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

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[localizedname]

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[security]

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

Queries value:

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

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

Queries value:

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

```
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}[precreate]
   Queries value:
db2c-424c-b029-7fe99a87c641}[stream]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
   Oueries value:
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
   Queries value:
folders[desktop]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[attributes]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[usedrophandler]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsforparsing]
   Oueries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
   Oueries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hideinwebview]
   Oueries value:
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                             HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
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]
                                              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus nonenum[\{20d04fe0-3aea-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-1069-a2d8-10
08002b30309d}1
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
   Queries value:
11e3-a68e-806e6f6e6963}[generation]
                                              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
   Queries value:
                                             HKLM\software\microsoft\com3[com+enabled]
   Queries value:
                                              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
   Oueries value:
                                              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
   Oueries value:
b8dc300d9f9d}\inprocserver32[1
   Queries value:
                                             HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
                                             HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                             HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Oueries value:
   Oueries value:
                                              HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
```

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

HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Queries value:

Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [separate process]$ 

Queries value:

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

Queries value:

 $HKLM \verb| software \verb| microsoft| windows \verb| current version \verb| policies \verb| explorer[nosimple startmenu]| \\$ 

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

Oueries value:

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

Queries value:

 $\label{thm:local_hidefile} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{thm:local_hidefileext} \end{tabular}$ 

Queries value:

Queries value:

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

Queries value:

 $\label{thm:local_equation} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [hideicons] \end{tabular}$ 

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[showsuperhidden]

Oueries value:

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

Queries value:

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [autocheck select]$ 

Oueries value:

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

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [show type overlay]$ 

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]
Oueries value: HKCR\folder[nevershowext]

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

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKCR\allfilesystemobjects[nevershowext]

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[category]$ 

Queries value:

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

Oueries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \cite{thm:hklk} for the label \cite{thm:hklk} and \cite{thm:hklk} for the label \ci$ 

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $HKLM \label{lem:hklm} White the latest and the la$ 65f9-4cf6-a03a-e3ef65729f3d}[streamresource]

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}$ 

folders[appdata]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[category]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[name]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parentfolder] Oueries value:

b587-4786-b4ef-bd1dc332aeae}[description]

Oueries value:

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parsingname]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b2b4a2b4b2ab4b2a2$ b587-4786-b4ef-bd1dc332aeae}[localizedname]

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ b587-4786-b4ef-bd1dc332aeae}[icon]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[security]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[streamresource]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

Oueries value:

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

Oueries value:

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

b587-4786-b4ef-bd1dc332aeae}[roamable]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[precreate]

Oueries value:

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]

Oueries value:

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[foldertypeid]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt Microsoft\windows\currentversion\explorer\user\ shell}$ Queries value:

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

Queries value:

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

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

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

Queries value:

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

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

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

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

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

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

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

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

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[icon]

Queries value:

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

Oueries value:

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

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

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

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

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

f20f-4863-afef-f87ef2e6ba25}[roamable]

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

Queries value:

 $HKLM \label{limits} Which windows \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current \cu$ f20f-4863-afef-f87ef2e6ba25}[stream]

Queries value:

f20f-4863-afef-f87ef2e6ba25}[publishexpandedpath]

Queries value:

f20f-4863-afef-f87ef2e6ba25}[attributes]

Queries value:

f20f-4863-afef-f87ef2e6ba25}[foldertypeid]

Queries value:

 $\label{thm:local_explorer} \begin{tabular}{ll} HKLM \end{tabular} Software \wow 6432 node \end{tabular} in cosoft \windows \current version \explorer \folder descriptions \end{tabular} \{c4aa340d-baseline \current version \end{tabular} and \current version \explorer \end{tabular} and \current version \end{tabular} and \curr$ f20f-4863-afef-f87ef2e6ba25}[initfolderhandler]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\user Queries value:

shell folders[common desktop]

Queries value:

 $HKLM \setminus Software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[turnoffspianimations]$ 

Sets/Creates value:

 $HKCU \ software \ head light \ getright to go \ customized apps [bb 32f7634f66faa 04bbed 52fd1a 61d36]$ Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[busypause]  $\label{thm:linear} \verb+HKCU\+ software\+ headlight\+ getrighttogo\+ shared config[file cache]$ Sets/Creates value: 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]