Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 37, Task ID: 145

Task ID: 145

Risk Level: 4

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

Processing Time: 61.07 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe"

Sample ID: 37
Type: basic
Owner: admin

Label: 7842072cea4eb57a03bdd00b54088404

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

File Type: PE32:win32:gui File Size: 807276 bytes

MD5: 7842072cea4eb57a03bdd00b54088404

SHA256: c1fe42986e89fd92ef404ed5ef57f650abb3eb526f77f3fb30a1167b1ab1791b

Description: None

Pattern Matching Results

2 PE: Nonstandard section

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

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

Process/Thread Events

Creates process: C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe

["C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\

Creates: C:\Users\Admin\AppData\Local\Temp\nsn1E7F.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nse2017.tmp

Creates: C:\Program Files (x86)

Creates: C:\Users\Admin\AppData\Local\Temp\nst2027.tmp

Creates: C:\Users
Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData
Creates: C:\Users\Admin\AppData\Local
Creates: C:\Users\Admin\AppData\Local\Temp

Creates: C:\Users\Admin\AppData\Local\Temp\nst2027.tmp\test.ini
Opens: C:\Windows\Prefetch\7842072CEA4EB57A03BDD00B54088-6F31F437.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\apphelp.dll

Opens: C:\Windows\Temp\7842072cea4eb57a03bdd00b54088404.exe

Opens: C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb C:\Windows\apppatch\AcGenral.dll Opens: Opens: C:\Windows\apppatch\AcLayers.dll C:\Windows\SysWOW64\sechost.dll Opens: Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\Windows\SysWOW64\winmm.dll C:\Windows\SysWOW64\samcli.dll Opens: C:\Windows\SysWOW64\msacm32.dll Opens: C:\Windows\SysWOW64\version.dll Opens:

Opens: C:\Windows\SysWOW64\userenv.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\SysWOW64\winspool.drv
Opens: C:\Windows\SysWOW64\mpr.dll
Opens: C:\Windows\SysWOW64\mpmmbase.dl

Opens: C:\Windows\SysWOW64\winmmbase.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Windows\SysWOW64\SHCore.dll

Opens: C:\Windows\SysWOW64\sfc.dll

```
C:\Windows\SysWOW64\sfc_os.dll
 Opens:
                          C:\windows\temp\7842072cea4eb57a03bdd00b54088404.exe.Config
 Opens:
 Opens:
                          C:\Windows\SysWOW64\msvcrt.dll
 Opens:
                          C:\Windows\SysWOW64\bcryptprimitives.dll
                          C:\Windows\SysWOW64\cryptbase.dll
 Opens:
                          C:\Windows\SysWOW64\sspicli.dll
 Opens:
                          C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\gdi32.dll
                          C:\Windows\SysWOW64\user32.dll
 Opens:
                          C:\Windows\SysWOW64\shlwapi.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\ole32.dll
                          C:\Windows\SysWOW64\oleaut32.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\advapi32.dll
                          C:\Windows\SysWOW64\shell32.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\iertutil.dll
 Opens:
                          C:\Windows\SysWOW64\wininet.dll
                          C:\Windows\SysWOW64\urlmon.dll
 Opens:
                          C:\Windows\SysWOW64\cfgmgr32.dll
 Opens:
                          C:\Windows\SysWOW64\devobj.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\setupapi.dll
 Opens:
                          C:\Windows\SysWOW64\imm32.dll
 Opens:
                          C:\Windows\SysWOW64\msctf.dll
 Opens:
                          C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
                          C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
 Opens:
                          C:\Windows\WindowsShell.Manifest
 Opens:
                          C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                          C:\
 Opens:
                          C:\Windows\SysWOW64\clbcatq.dll
                          C:\Windows\SysWOW64\propsys.dll
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
 Opens:
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db
 Opens:
                          C:\Windows\SysWOW64\desktop.ini
 Opens:
                          C:\Users\Admin\Desktop\desktop.ini
                          C:\Users
 Opens:
 Opens:
                          C:\Users\Admin
 Opens:
                          C:\Users\Admin\AppData
 Opens:
                          C:\Users\Admin\AppData\Local
 Opens:
                          C:\Users\Admin\AppData\Local\Temp
                          C: \verb|\Users| Admin\\| AppData\\| Local\\| Temp\\| nsn1E7F.tmp\\|
 Opens:
 Opens:
                          C:\Program Files (x86)\desktop.ini
 Opens:
                          C:\Users\Admin\AppData\Local\Temp\nst2027.tmp
 Opens:
                          C:\Windows\SysWOW64\riched20.dll
 Opens:
                          C:\Windows\SysWOW64\usp10.dll
 Opens:
                          C:\Windows\SysWOW64\msls31.dll
 Opens:
                          C:\Windows\Fonts\tahoma.ttf
 Opens:
                          C:\Windows\win.ini
 Opens:
                          C:\Windows\SysWOW64\UxTheme.dll.Config
 Opens:
                          C:\Windows\Fonts\StaticCache.dat
 Opens:
                          C:\Windows\Fonts\micross.ttf
 Writes to:
                          C:\Users\Admin\AppData\Local\Temp\nse2017.tmp
 Writes to:
                          C:\Users\Admin\AppData\Local\Temp\nst2027.tmp\test.ini
 Reads from:
                          C:\Users\Admin\Desktop\desktop.ini
 Reads from:
                          C: \verb|\windows\Temp\7842072cea4eb57a03bdd00b54088404.exe|
 Reads from:
                          C:\Users\Admin\AppData\Local\Temp\nse2017.tmp
                          C:\Program Files (x86)\desktop.ini
 Reads from:
 Reads from:
                          C:\Windows\win.ini
 Reads from:
                          C:\Windows\Fonts\StaticCache.dat
 Deletes:
                          C: \verb|\Users| Admin\\| AppData\\| Local\\| Temp\\| nsn1E7F.tmp\\|
 Deletes:
                          C:\Users\Admin\AppData\Local\Temp\nst2027.tmp
Windows Registry Events
 Opens key:
                          HKLM\software\microsoft\wow64
 Opens key:
                          HKLM\system\currentcontrolset\control\terminal server
 Opens key:
                          HKLM\system\currentcontrolset\control\safeboot\option
 Opens key:
                          {\tt HKLM \ } system \verb|\ current control \ \\ srp \verb|\ gp \ \\ dll
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                          HKLM\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                          HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                          HKLM\system\currentcontrolset\control\nls\customlocale
 Opens key:
                          HKLM\system\currentcontrolset\control\nls\language
 Opens key:
                          HKLM\system\currentcontrolset\control\mui\uilanguages
 Opens key:
                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
 Opens key:
                          HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
 Opens key:
                          HKLM\software\wow6432node\policies\microsoft\mui\settings
 Opens key:
                          HKLM\software\policies\microsoft\mui\settings
 Opens key:
```

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

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration Opens key: HKCU\control panel\desktop Opens key: HKCU\control panel\desktop\muicached $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$ Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} in the constant \end{tabular} and \e$ Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file protection HKLM\software\policies\microsoft\windows nt\windows file protection Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy Opens key: HKLM\system\currentcontrolset\control\lsa Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\gre_initialize Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing Opens key: Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup Opens kev: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens kev: HKLM\system\currentcontrolset\control\nls\sorting\ids Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 7842072 cea 4eb 57a 03bdd 00b 54088404. exemple \ applications \ applicat$ HKCU\software\classes\ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder $HKCU \ software \ `microsoft \ `windows \ `current version \ `explorer \ clsid \ '\{20d04fe0-microsoft \ 'windows \ 'current \ 'explorer' \ 'clsid \ 'all \ 'explorer' \ 'clsid' \ 'explorer' \ 'exp$ Opens key: 3aea-1069-a2d8-08002b30309d}\shellfolder Opens kev: a2d8-08002b30309d}\shellfolder Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\inprocserver32

Opens key:

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ cpc \ volume \ \{d5291c64-7c88-4c14, d5291c64-7c88-4c14, d5291c64-7c88-4c140, d5291c64-7c88-4c1464-7c88-4c140, d5291c64-7c88-4c140, d5291c64-7c88-4c140, d5291c6$

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

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

4442-804e-409d6c4515e9} Opens key:

409d6c4515e9} Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus explorer$

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

```
Opens key:
                                                        HKCU\software\policies\microsoft\windows\explorer
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\advanced
    Opens key:
                                                        HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034fd-6caa-4954-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-407034-ac3f-4070
97a27216f98a}\inprocserver32
    Opens key:
                                                        HKCU\software\classes\directory
    Opens key:
                                                        HKCR\directory
    Opens key:
                                                        HKCU\software\classes\directory\shellex\iconhandler
    Opens key:
                                                        HKCR\directory\shellex\iconhandler
    Opens key:
                                                        HKCU\software\classes\folder
    Opens kev:
                                                        HKCR\folder
    Opens key:
                                                        HKCU\software\classes\folder\shellex\iconhandler
                                                        HKCR\folder\shellex\iconhandler
    Opens key:
    Opens key:
                                                        HKCU\software\classes\allfilesystemobjects
    Opens key:
                                                        HKCR\allfilesystemobjects
                                                        HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
    Opens key:
    Opens key:
                                                        HKCR\allfilesystemobjects\shellex\iconhandler
    Opens key:
                                                        HKCU\software\classes\directory\docobject
    Opens key:
                                                        HKCR\directory\docobject
    Opens key:
                                                        HKCU\software\classes\folder\docobject
    Opens key:
                                                        HKCR\folder\docobject
    Opens key:
                                                        HKCU\software\classes\allfilesystemobjects\docobject
    Opens key:
                                                        HKCR\allfilesystemobjects\docobject
    Opens key:
                                                        HKCU\software\classes\directory\browseinplace
    Opens key:
                                                        HKCR\directory\browseinplace
    Opens key:
                                                        HKCU\software\classes\folder\browseinplace
    Opens key:
                                                        HKCR\folder\browseinplace
    Opens key:
                                                        HKCU\software\classes\allfilesystemobjects\browseinplace
    Opens key:
                                                        HKCR\allfilesystemobjects\browseinplace
    Opens key:
                                                        HKCU\software\classes\directory\clsid
    Opens key:
                                                        HKCR\directory\clsid
    Opens key:
                                                        HKCU\software\classes\folder\clsid
    Opens key:
                                                        HKCR\folder\clsid
    Opens key:
                                                        HKCU\software\classes\allfilesystemobjects\clsid
    Opens kev:
                                                        HKCR\allfilesystemobjects\clsid
    Opens key:
                                                        HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32
    Opens key:
                                                        HKLM\software\microsoft\com3
    Opens key:
                                                        HKLM\software\microsoft\windowsruntime\clsid
    Opens key:
                                                        HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
    Opens key:
                                                        HKCR\activatableclasses\clsid
    Opens key:
                                                        HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
    Opens key:
                                                        HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
    Opens key:
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
    Opens key:
                                                        HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
    Opens key:
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
    Opens key:
                                                        HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key:
b8dc300d9f9d}\inprocserver32
                                                        HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key:
b8dc300d9f9d}\inprochandler32
    Opens key:
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler32
    Opens key:
                                                        HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprochandler
                                                        HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
    Opens key:
b8dc300d9f9d}\inprochandler
                                                        HKLM \setminus system \setminus current control \setminus device classes \setminus \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6b
    Opens key:
94f2-00a0c91efb8b}
    Opens key:
```

Opens key:

db2c-424c-b029-7fe99a87c641}

Opens key:

 $HKLM \label{lem:hklm} Which is the latest and the$ db2c-424c-b029-7fe99a87c641}\propertybag

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens kev:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session info \ 1\ known folders$

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

folders Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-16der \ and \ baselines \ explorer \ e$

```
b587-4786-b4ef-bd1dc332aeae}
    Opens kev:
b587-4786-b4ef-bd1dc332aeae}\propertybag
HKLM \label{lem:hklm} Which is the latest and the
65f9-4cf6-a03a-e3ef65729f3d}
    Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
    Opens kev:
0e22-4760-9afe-ea3317b67173}
    Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
                                                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
                                                          HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
    Opens key:
1923240461-1905901954-2556564120-1001
   Opens key:
                                                          HKLM \ system \ current control \ device classes \ \ \{53f5630d-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b6bf-11d0-b
94f2-00a0c91efb8b}\properties
    Opens key:
11e3-be65-806e6f6e6963}\
    Opens kev:
                                                          HKLM\software\wow6432node\evillvrics
    Opens key:
c1bf-494e-b29c-65b732d3d21a}
    Opens key:
c1bf-494e-b29c-65b732d3d21a}\propertybag
a0fb-4bfc-874a-c0f2e0b9fa8e}
    Opens key:
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
    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:
Opens key:
                                                          HKLM\software\wow6432node\microsoft\ctf\
                                                          HKCU\software\microsoft\windows nt\currentversion\windows
    Opens kev:
    Opens key:
                                                          HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
    Opens key:
                                                          HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\datastore\_v1.0|
    Opens key:
                                                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
                                                          HKLM\software\microsoft\windows
    Opens key:
\verb| nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2| \\
    Opens key:
                                                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
                                                          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Oueries value:
    Queries value:
                                                          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                          HKLM\system\currentcontrolset\control\nls\customlocale[empty]
    Oueries value:
    Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
    Queries value:
    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]
    Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
                                                          HKLM\system\currentcontrolset\control\nls\sorting\versions[]
    Oueries value:
    Queries value:
                                                          HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
                                                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:
```

HKLM\software\policies\microsoft\windows nt\windows file Oueries value:

protection[knowndlllist]

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

HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Oueries value:

Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Queries value: $\verb|nt\currentversion\compatibility32[7842072cea4eb57a03bdd00b54088404]| \\$ Oueries value: HKLM\software\wow6432node\microsoft\windows

```
nt\currentversion\windows[loadappinit_dlls]
                                                            HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Oueries value:
    Queries value:
                                                            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
    Queries value:
                                                            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
    Queries value:
                                                            HKLM\software\microsoft\ole[aggressivemtatesting]
    Queries value:
                                                            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
                                                             HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Queries value:
                                                            HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
    Oueries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
    Queries value:
                                                            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
    Oueries value:
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
    Oueries value:
options\dllnxoptions[7842072cea4eb57a03bdd00b54088404.exe]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
HKLM\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]
                                                            HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
    Oueries value:
                                                            HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
    Queries value:
    Oueries value:
                                                            HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Oueries value:
                                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
                                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
    Queries value:
08002b30309d}\shellfolder[foldervalueflags]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}1
    Queries value:
                                                            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
    Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus volume \setminus \{d5291c64-7c88-five a content version \setminus cpc \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc \setminus cpc \setminus cpc \setminus cpc \setminus cpc \setminus cpc \setminus volume \setminus \{d5291c64-five a content version \setminus cpc 
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c88-4c64-7c
11e3-be65-806e6f6e6963}[generation]
                                                            HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
    Oueries value:
409d6c4515e9}[drivemask]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
                                                            HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                                            HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Queries value:
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
    Oueries value:
```

```
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
     Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
     Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
     Oueries value:
\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite[iconsonly]]{thm:local_explorer} \end{tabular} \begin{tabular}{ll} HKCU \software \microsoft \windows \cite[iconsonly]]{thm:local_explorer} \begin{tabular}{ll} HKCU \software \microsoft \windows \cite[iconsonly]]{thm:local_explorer} \begin{tabular}{ll} HKCU \software \windows \cite[iconsonly]]{thm:local_explorer} \begin{tabular}{ll} HKCU \software \windows \window
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
     Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
     Oueries value:
                                                                     HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
 97a27216f98a}\inprocserver32[]
                                                                     HKCR\directory[docobject]
     Oueries value:
     Queries value:
                                                                     HKCR\folder[docobject]
                                                                     HKCR\allfilesystemobjects[docobject]
     Oueries value:
     Queries value:
                                                                     HKCR\directory[browseinplace]
     Queries value:
                                                                     HKCR\folder[browseinplace]
                                                                     HKCR\allfilesystemobjects[browseinplace]
     Oueries value:
                                                                     HKCR\directory[isshortcut]
     Oueries value:
     Oueries value:
                                                                     HKCR\folder[isshortcut]
     Queries value:
                                                                     HKCR\allfilesystemobjects[isshortcut]
     Queries value:
                                                                     HKCR\directory[alwaysshowext]
     Queries value:
                                                                     HKCR\directory[nevershowext]
     Queries value:
                                                                     HKCR\folder[nevershowext]
                                                                     HKCR\allfilesvstemobjects[nevershowext]
     Oueries value:
                                                                     HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
     Queries value:
 a6bb2164fbd0}\inprocserver32[]
     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[]
                                                                    HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
     Oueries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
     Queries value:
                                                                    HKLM\software\microsoft\ole[maxsxshashcount]
     Oueries value:
db2c-424c-b029-7fe99a87c641}[category]
     Queries value:
db2c-424c-b029-7fe99a87c641}[name]
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bfcc3a-b4bf
db2c-424c-b029-7fe99a87c641}[parentfolder]
     Queries value:
db2c-424c-b029-7fe99a87c641}[description]
     Oueries value:
db2c-424c-b029-7fe99a87c641}[relativepath]
     Queries value:
db2c-424c-b029-7fe99a87c641}[parsingname]
     Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
db2c-424c-b029-7fe99a87c641}[infotip]
     Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ f
 db2c-424c-b029-7fe99a87c641}[localizedname]
     Oueries value:
db2c-424c-b029-7fe99a87c641}[icon]
     Queries value:
db2c-424c-b029-7fe99a87c641}[security]
db2c-424c-b029-7fe99a87c641}[streamresource]
     Queries value:
db2c-424c-b029-7fe99a87c641}[streamresourcetype]
     Oueries value:
db2c-424c-b029-7fe99a87c641}[localredirectonly]
     Oueries value:
db2c-424c-b029-7fe99a87c641}[roamable]
```

 $\label{thm:local-soft-windows} Label{thm:local-windows} In the description of the descr$

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

Oueries value:

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

Queries value:

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

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

Oueries value:

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

Oueries value:

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

Queries value:

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

folders[desktop]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[category]

b587-4786-b4ef-bd1dc332aeae}[name]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parentfolder]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[description]

Oueries value:

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parsingname]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

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

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{1b3ea5dc-1b4e$ b587-4786-b4ef-bd1dc332aeae}[icon]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[security]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[streamresource]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

Oueries value:

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

b587-4786-b4ef-bd1dc332aeae}[roamable]

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[stream]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]

Queries value:

b587-4786-b4ef-bd1dc332aeae}[attributes]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[foldertypeid]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]

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

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 6569-4cf6-a03a-e3ef65729f3d \category \]$

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \descriptions \folds folder \descriptions \folds folder \descriptions \folds folder \descriptions \folds folds folder \descriptions \folds folds folder \descriptions \folds folds folds \descriptions \folds folds \descriptions \folds folds \descriptions \folds \descriptions \descriptions \folds \descriptions \folds \descriptions \folds \descriptions \descriptions \folds \descriptions \folds \descriptions \folds \folds \descriptions \folds \fo$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folds \folds \fold$

Queries value:

 $\label{local-ham} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[publishexpandedpath]$

Oueries value

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folder \folds folds folder \folds folder \folds folder \folds folder \folds folds folder \folds folder \folds folds folder \folds folds folder \folds folds folder \folds folds folds folder \folds folds folds$

Oueries value:

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

Queries value:

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

folders[appdata]

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.00} \cite{1.00} \cite{1.00} \end{tikzpicture} $$ -0e22-4760-9afe-ea3317b67173 \cite{1.00} \cite{1.$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [name]$

Oueries value

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[parentfolder]$$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [relative path]$

Queries value

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

Oueries value:

0e22-4760-9afe-ea3317b67173}[infotip]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [localized name]$

Queries value:

 $H\dot{L}M\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [security]$

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{2} e6c858f-0e22-4760-9 af e-ea3317 b67173 \footnote{1}{2} [stream resource]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [stream resource type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [local redirectionly]$

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [folder type id]$

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]

Oueries value:

 $HKCU \ software \ `microsoft \ `windows \ current version \ explorer \ `mountpoints2 \ cpc \ volume \ \{d5291c63-7c88-11e3-be65-806e6f6e6963\} \ [data]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\category\]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{2000} folder \cite{20000} folder \cite{2000} folder \cite{2000} folder \cite{2000} folder \cite{2000} folder \cite{2000} folder \cite{2000} folder \$

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{200} \folder \c$

Queries value

 $\label{thm:local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[relativepath]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [parsing name]$

Queries value:

 $\label{thm:local-ham} $HKLM \cdot oftware \cdot wow 6432 node \cdot irrentversion \cdot explorer \cdot folder descriptions \cdot \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [infotip]$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localizedname]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\[security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [stream resource]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [stream resource type]$

Oueries value

 $\label{thm:local-condition} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqref{folderdescriptions} and the software\eqref{folderdescriptions}. The software\eqref{folderdescriptions} are the software\eqref{folderdescriptions} and the software\eqref{folderdescriptions} are the software\eqref{folderdes$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [roamable]$

Oueries value:

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

Oueries value

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{200} folder \cite{200} fo$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [publish \ expanded path]$

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{local-bound} \end{substants} $$ 1bf-494e-b29c-65b732d3d21a \cite{local-bound} \cite{local-bound} \end{substants} $$ 1bf-494e-b29c-65b732d3d21a \cite{local-bound} \cite{$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [initfolder handler]$

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} des$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [name]$

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder-a0fb-4bfc-874a-c0f2e0b9fa8e\[parentfolder\]$

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [relative path]$

Oueries value:

 $\label{thm:local-ham} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e)\currentpersion\currentpersion\explorer\folderdescriptions\f(7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e)\currentpersion\currentpersi$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [localized name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}[icon]$

Oueries value:

Queries value:

 $\label{thm:local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e)\[[streamresource] \]$

Queries value

Queries value:

 $\label{local-reduced-soft-windows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\[local\creduced]\]$

Oueries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}[stream]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} a 0 fb-4 bfc-874 a-c 0 f2 e 0 b 9 fa 8 e \footnote{1.5} [publish expanded path]$

Queries value:

```
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \ descriptions \ explorer \ folder \ descriptions \ explorer \ folder 
a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
     Queries value:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-descriptions\} \\ folde
a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
     Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag[foldersdependenton]
                                                                                  Oueries value:
     Queries value:
                                                                                   HKLM\system\currentcontrolset\control\nls\language groups[1]
     Oueries value:
                                                                                   HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
     Queries value:
                                                                                  HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
     Oueries value:
                                                                                  HKCU\software\microsoft\windows nt\currentversion\windows[dragdelav]
     Queries value:
                                                                                   HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
     Queries value:
                                                                                   HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
                                                                                  HKCU\software\microsoft\windows
     Oueries value:
 nt\currentversion\windows[scrollinterval]
     Oueries value:
HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                                                                                   HKLM\software\microsoft\windows
     Oueries value:
\verb|nt\currentversion\languagepack\datastore\_v1.0[datafilepath]|
                                                                                  HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
     Queries value:
                                                                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
     Oueries value:
                                                                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
                                                                                  HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
                                                                                  HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
     Queries value:
                                                                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                                                                  HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
     Queries value:
                                                                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
     Queries 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:
\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|
     Queries value:
                                                                                  HKLM\software\microsoft\windows
```

nt\currentversion\languagepack\surrogatefallback[plane12]

nt\currentversion\languagepack\surrogatefallback[plane13]

nt\currentversion\languagepack\surrogatefallback[plane14]

nt\currentversion\languagepack\surrogatefallback[plane15]

nt\currentversion\languagepack\surrogatefallback[plane16]

Queries value:

Queries value:

Oueries value:

Oueries value:

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows