Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 217

Task ID: 217 Risk Level: 4

Date Processed: 2016-04-28 12:53:12 (UTC)

Processing Time: 5.49 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe"

Sample ID: 54
Type: basic
Owner: admin

Label: 607c7d18e490c5b56e91c74a29ae3e0a

Date Added: 2016-04-28 12:44:55 (UTC)

File Type: PE32:win32:gui File Size: 106104 bytes

MD5: 607c7d18e490c5b56e91c74a29ae3e0a

SHA256: 006257143f3aa20ebc8a51441005feee0cce6d81bca404356d3c1cb657345b9e

Description: None

Pattern Matching Results

HTTP connection - response code 404 (file not found) [HTTP, GET, POST, web, network, response code]

2 PE: Nonstandard section

3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]

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\607c7d18e490c5b56e91c74a29ae3e0a.exe

["C:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe"]

Terminates process: C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \Sessions\1\BaseNamedObjects_!MSFTHISTORY!_

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet

files!content.ie5! Creates mutex:

 $\verb|\Sessions|1| Base Named Objects \verb|\c:!users!| admin!| appdata!| roaming!| microsoft!| windows!| cookies!| admin!| appdata!| roaming!| microsoft!| windows!| cookies!| admin!| appdata!| roaming!| microsoft!| windows!| cookies!| admin!| appdata!| appdata!| admin!| appdata!| appdata!|$

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile
Creates event: \KernelObjects\MaximumCommitCondition
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\BFE_Notify_Event_{47bfaf7d-1a09-4f21-92b2-

e94e72bafd33}

File System Events

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

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

Creates: C:\Users\Admin\AppData\Local\Temp\nsu7FA.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsu7FB.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp

Creates: C:\Users
Creates: C:\Users\Admin
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\nsu7FC.tmp\System.dll Creates: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\zplugins.dll

Creates: C:\Users\Admin\AppData\Local\Temp\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files

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

Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\result.txt
Opens: C:\Windows\Prefetch\607C7D18E490C5B56E91C74A29AE3-1B2D8BFB.pf

Opens: C:\Windows

```
C:\Windows\System32\wow64.dll
  Opens:
                                      C:\Windows\System32\wow64win.dll
  Opens:
  Opens:
                                      C:\Windows\System32\wow64cpu.dll
                                      C:\Windows\system32\wow64log.dll
  Opens:
  Opens:
                                      C:\Windows\SysWOW64
  Opens:
                                      C:\Windows\SysWOW64\sechost.dll
                                      C:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe.Local\
  Opens:
                                      C:\Windows\winsxs\x86_microsoft.windows.common-
  Opens:
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
                                      C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
  Opens:
                                      C:\windows\temp\VERSION.dll
  Opens:
                                      C:\Windows\SysWOW64\version.dll
                                      C:\Windows\SysWOW64\imm32.dll
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\rpcss.dll
                                      C:\Windows\SysWOW64\uxtheme.dll
  Opens:
  Opens:
                                      C:\windows\temp\SHFOLDER.DLL
  Opens:
                                      C:\Windows\SysWOW64\shfolder.dll
  Opens:
                                      C:\Windows\Globalization\Sorting\SortDefault.nls
                                      C:\Windows\SysWOW64\shell32.dll
  Opens:
  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\WindowsShell.Manifest
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\propsys.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
  Opens:
                                      C:\windows\temp\ntmarta.dll
  Opens:
                                      C:\Windows\SysWOW64\ntmarta.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
  Opens:
                                      C:\Users\Admin\Desktop\desktop.ini
  Opens:
                                      C:\windows\temp\profapi.dll
  Opens:
                                      C:\Windows\SysWOW64\profapi.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nsu7FA.tmp
  Opens:
                                      C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp
  Opens:
                                      C:\Users
                                      C:\Windows\SysWOW64\en-US\setupapi.dll.mui
  Opens:
  Opens:
                                      C:\Users\Admin
  Opens:
                                      C:\Users\Admin\AppData
                                      C:\Users\Admin\AppData\Local
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\System.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\zplugins.dll
                                      \label{local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-loc
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\wininet.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Roaming
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:
                                      C:\windows\temp\dnsapi.DLL
  Opens:
                                      C:\Windows\SysWOW64\dnsapi.dll
  Opens:
                                      C:\windows\temp\iphlpapi.DLL
                                      C:\Windows\SysWOW64\IPHLPAPI.DLL
  Opens:
  Opens:
                                      C:\windows\temp\WINNSI.DLL
  Opens:
                                      C:\Windows\SysWOW64\winnsi.dll
  Opens:
                                      C:\windows\temp\RASAPI32.dll
  Opens:
                                      C:\Windows\SysWOW64\rasapi32.dll
                                      C:\windows\temp\rasman.dll
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\rasman.dll
                                      C:\windows\temp\rtutils.dll
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\rtutils.dll
  Opens:
                                      C:\ProgramData\Microsoft\Network\Connections\Pbk\
  Opens:
                                      C:\Windows\SysWOW64\ras
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
  Opens:
  Opens:
                                      C:\windows\temp\sensapi.dll
```

C:\Windows\SysWOW64\SensApi.dll Opens: C:\Windows\SysWOW64\nlaapi.dll Opens: C:\windows\temp\rasadhlp.dll Opens: Opens: C:\Windows\SysWOW64\rasadhlp.dll Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL C:\Windows\SysWOW64\wship6.dll Opens: Opens: C:\windows\temp\dhcpcsvc6.DLL C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\Windows\System32\drivers\etc\hosts Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL

C:\Users\Admin\AppData\Local\Temp\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C Opens:

Opens: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\result.txt

C:\Users\Admin\AppData\Local\Temp\nsu7FB.tmp Writes to:

Writes to: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\System.dll Writes to: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\zplugins.dll

Reads from: C:\Users\Admin\Desktop\desktop.ini

Reads from: C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe

C:\Users\Admin\AppData\Local\Temp\nsu7FB.tmp Reads from: C:\Windows\System32\drivers\etc\hosts Deletes: C:\Users\Admin\AppData\Local\Temp\nsu7FA.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\result.txt Deletes: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\System.dll Deletes: C:\Users\Admin\AppData\Local\Temp\nsu7FC.tmp\zplugins.dll

Network Events

Reads from:

dl.distromatic.com DNS query: DNS query: utrack.n.distromatic.com

DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.39$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.176$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.203$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.19$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.83$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.221$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.106$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.98$ DNS response: utrack.n.distromatic.com ⇒ 52.73.93.66 DNS response: utrack.n.distromatic.com ⇒ 52.87.82.229

Connects to: 54.230.144.39:80 52.73.93.66:80 Connects to: Sends data to: 8.8.8.8:53

Sends data to: d2624xgal0u1e4.cloudfront.net:80 (54.230.144.39)

Sends data to: utrack.n.distromatic.com:80 (52.73.93.66)

Receives data from: 8.8.8.8:53

Receives data from: d2624xgal0u1e4.cloudfront.net:80 (54.230.144.39)

Receives data from: utrack.n.distromatic.com:80 (52.73.93.66)

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings

Creates key: HKLM\software\wow6432node\microsoft\tracing

Creates key:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32

Creates kev:

Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\connections

Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

Creates key: HKLM\svstem\currentcontrolset\services\tcpip\parameters Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride] Deletes value:

HKCU\software\microsoft\windows\currentversion\internet

settings[autoconfigurl]

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

Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\software\microsoft\wow64

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

execution options

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

Opens key:

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

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

Opens key: Opens key: HKLM\svstem\currentcontrolset\control\nls\language

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

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens kev:

HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

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:

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

HKLM\ Opens kev:

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

nt\currentversion\diagnostics

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

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

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

Opens kev: HKLM\software\microsoft\ole\tracing

Opens key:

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

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

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 607c7d18e490c5b56e91c74a29ae3e0a. exemple \ descriptions \$

HKLM\software\wow6432node\microsoft\oleaut Opens kev:

HKCU\software\classes\ Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

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

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

Opens kev:

a2d8-08002b30309d}\shellfolder

Opens key: $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+policies\+nonenum$

Opens kev:

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

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume Opens key:

 $HKCU \setminus software \setminus irrelation \cdot explorer \setminus mountpoints \\ 2 \setminus cpc \setminus volume \setminus \{8063a3d4-8213-42d1$

11e3-a68e-806e6f6e6963}\

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

HKCR\drive\shellex\folderextensions Opens key:

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\$ Opens key:

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

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

Opens key: HKCR\directory\curver Opens key: HKCR\directory\

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

```
Opens key:
                                                                                     HKCU\software\classes\allfilesystemobjects
      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
                                                                                     HKCU\software\classes\folder\docobject
      Opens key:
                                                                                     HKCR\folder\docobject
      Opens key:
      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
                                                                                     HKCR\folder\browseinplace
      Opens key:
      Opens key:
                                                                                     HKCU\software\classes\allfilesystemobjects\browseinplace
      Opens key:
                                                                                     HKCR\allfilesystemobjects\browseinplace
                                                                                     HKCU\software\classes\directory\clsid
      Opens kev:
      Opens key:
                                                                                     HKCR\directory\clsid
      Opens key:
                                                                                     HKCU\software\classes\folder\clsid
      Opens key:
                                                                                     HKCR\folder\clsid
      Opens key:
                                                                                     HKCU\software\classes\allfilesystemobjects\clsid
      Opens key:
                                                                                     HKCR\allfilesystemobjects\clsid
      Opens kev:
Opens key:
db2c-424c-b029-7fe99a87c641}
      Opens key:
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}\propertybag
                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
      Opens kev:
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders
      Opens key:
                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
      Opens key:
                                                                                     HKLM\software\microsoft\com3
                                                                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
      Opens kev:
b8dc300d9f9d}
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
      Opens key:
                                                                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
      Opens key:
b8dc300d9f9d}\treatas
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\ \treatas
      Opens key:
                                                                                     HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
      Opens kev:
b8dc300d9f9d}\progid
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
      Opens kev:
                                                                                     HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
      Opens key:
      Opens key:
                                                                                     HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
                                                                                     Opens key:
b8dc300d9f9d}\progid
                                                                                     \label{lem:hkcr} $$ HKCR\clsid_{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} \rightarrow \clsid_{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} $$
      Opens key:
                                                                                     HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50
      Opens kev:
b8dc300d9f9d}\inprocserver32
      Opens key:
                                                                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32
                                                                                     HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 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
      Opens key:
                                                                                     HKLM \setminus system \setminus current control \\ \setminus lsa \setminus access providers
      Opens kev:
                                                                                     HKLM\svstem\currentcontrolset\services\ldap
      Opens key:
HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| \verb|\windows \verb|\currentversion| explorer \verb|\knownfoldersettings| for the property of the prop
     Opens key:
HKLM \label{lem:hklm} White the latest and the la
b587-4786-b4ef-bd1dc332aeae}
     Opens kev:
b587-4786-b4ef-bd1dc332aeae}\propertybag
     Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}
     Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
     Opens kev:
```

 $Opens \ key: \\ HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1.5} \ footnote{1.5} \ footn$

0e22-4760-9afe-ea3317b67173}

0e22-4760-9afe-ea3317b67173}\propertybag HKLM\software\wow6432node\microsoft\windows Opens kev: nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001 Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001 Opens key: HKLM\system\currentcontrolset\control\cmf\config HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\setup $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion||$ Opens key: HKLM\software\wow6432node\microsoft\rpc Opens key: Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\$ Opens key: HKLM\system\setup HKLM\software\wow6432node\policies\microsoft\windows nt\rpc Opens key: Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\sqmclient\windows HKLM\software\microsoft\samclient\windows Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions Opens key: 11e3-a68e-806e6f6e6963}\ HKLM\system\currentcontrolset\services\crypt32 Opens kev: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings

Opens key:

HKCU\software\policies\microsoft\windows\currentversion\internet

settings

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version \label{thm:local_hammon} internet settings \end{tabular}$ Opens key:

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

HKCU\software Opens key:

Opens key: HKLM\software\wow6432node

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

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

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main

Opens key: HKLM\software\policies\microsoft\internet explorer\main Opens key: HKLM\software\wow6432node\policies\microsoft\internet

explorer\main\featurecontrol

HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens kev: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key:

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol

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

explorer\main\featurecontrol

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

settings\5.0\cache

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

settings\5.0\cache Opens kev:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content

Opens key:

settings\5.0\cache\content

Opens key:

33be-4251-ba85-6007caedcf9d}

Opens kev:

33be-4251-ba85-6007caedcf9d}\propertybag

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b1$ 6fba-4fcf-9d55-7b8e7f157091}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785-b2786, \ b2786, \ b2$ 6fba-4fcf-9d55-7b8e7f157091}\propertybag

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

c0e9-4171-908e-08a611b84ff6}

Opens key:

c0e9-4171-908e-08a611b84ff6}\propertybag

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

settings\5.0\cache\history

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

settings\5.0\cache\history

Opens kev:

```
b784-432e-a781-5a1130a75963}
 Opens kev:
b784-432e-a781-5a1130a75963}\propertybag
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
 Opens key:
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\5.0\cache\extensible cache\feedplat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\iecompat
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature allow long international filenames
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                         HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619

HKLM\software\wow6432node\microsoft\internet

Opens key:

explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828 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\00f84a46 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens key: Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: 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: 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: Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\wpad}} \\$ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature return failed connect content kb942615 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_mime_handling Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling Opens key: HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32 Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasmancs$ Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist HKLM\software\microsoft\sqmclient\windows\disabledprocesses\ Opens key: Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\

Opens key: HKU\
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient

HKLM\system\currentcontrolset\control\sqmservicelist

Opens key:

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

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

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

nt\dnsclient\dnspolicyconfig

Opens kev: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig

Opens key:

HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig HKLM\system\currentcontrolset\services\winsock\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

HKLM\system\currentcontrolset\services\winsock\setup migration\providers Opens key:

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

Opens key: ${\tt HKLM \ } system \ \verb| current control set \ \verb| services \ \verb| winsock \ \verb| setup \ | \ setup \ | \$

migration\providers\tcpip6

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

HKLM\software\policies\microsoft\system\dnsclient Opens kev:

Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache

Opens key:

 $HKLM \land system \land current control set \land services \land tcpip6 \land parameters \land (22873b3e-c4d3-495a-8165-d3495a-d49$

e1e01c1f69b5}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces

Opens kev:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-

Opens key:

 $HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{846ee 342-7039-11de-9d20-11de-$

806e6f6e6963}

Opens kev:

806e6f6e6963}

Opens key:

127795cce47a}

Opens kev: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-

65fee5bae0b1}

HKLM\system\currentcontrolset\services\tcpip\linkage Opens key: Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions

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

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc mage file execution} \\$ Oueries value:

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

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

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

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

us[alternatecodepage]

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

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

Oueries value:

 $HKLM \label{lem:hklm} Wow 6432 node \verb|microsoft| windows \verb|currentversion| side by side [preferex ternal manifest]| and the leminary of the$

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

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

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\gre_initialize[disablemetafiles] Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[607c7d18e490c5b56e91c74a29ae3e0a] HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\windows[loadappinit dlls]

HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value:

Queries value:

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

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

Oueries value:

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

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

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value:

Oueries value:

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

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

08002b30309d}\shellfolder[attributes]

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

```
08002b30309d}\shellfolder[callforattributes]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
  Oueries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
  Queries value:
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[queryforinfotip]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                      HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
  Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-1069-a2d8-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3aea-4064e0-3a
08002b30309d}1
  Oueries 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-
  Oueries value:
409d6c4515e9}[drivemask]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
\label{thm:local_explorer} HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[nowebview]
  Queries 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]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                     HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
  Oueries value:
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{linear} hidefile ext] \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
\label{lem:hkcu} \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]
                                     HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Oueries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Oueries value:
Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [autocheck select]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
```

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

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]

 $\label{lem:continuous} Queries \ value: \\ HKCR \ all filesystem objects [is short cut]$

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

Oueries value: HKCR\folder[nevershowext]

Queries value: HKCR\allfilesystemobjects[nevershowext]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma(b4bfcc3a-db2c-424c-b029-7fe99a87c641)\[parsing name]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Ougries value

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

folders[desktop]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[]

Oueries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[threadingmodel]

Oueries value: HKLM\software\microsoft\ole[maxsxshashcount]

Queries value:

 $HKLM \setminus system \setminus current control \\ \ \mid sa \setminus access providers [martaextension]$

HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder] Queries value: ${\tt HKLM \ } system \verb| current control set \verb| services \verb| ldap [use host name as alias]|$ Oueries value:

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[category]

Queries value:

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

Queries value:

b587-4786-b4ef-bd1dc332aeae}[parentfolder]

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

b587-4786-b4ef-bd1dc332aeae}[relativepath]

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

b587-4786-b4ef-bd1dc332aeae}[infotip]

b587-4786-b4ef-bd1dc332aeae}[localizedname]

b587-4786-b4ef-bd1dc332aeae}[icon]

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

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

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

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

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-16b4e$ b587-4786-b4ef-bd1dc332aeae}[precreate]

b587-4786-b4ef-bd1dc332aeae}[stream]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-16b4e$ b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]

b587-4786-b4ef-bd1dc332aeae}[attributes]

Queries value:

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

b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]

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

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Oueries value

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

Queries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[folder typeid]$

Queries value:

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

Queries value:

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

folders[appdata]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{$5e6c858f-0e22-4760-9afe-ea3317b67173} \ [name]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{ali$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{localized halo} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder descriptions \folder \folder descriptions \folder \$

Queries value:

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

Queries value:

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

Queries value:

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

```
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
 Oueries value:
0e22-4760-9afe-ea3317b67173}[localredirectonly]
 Queries value:
0e22-4760-9afe-ea3317b67173}[roamable]
 Oueries value:
0e22-4760-9afe-ea3317b67173}[precreate]
 Queries value:
0e22-4760-9afe-ea3317b67173}[stream]
 Queries value:
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
0e22-4760-9afe-ea3317b67173}[attributes]
0e22-4760-9afe-ea3317b67173}[foldertypeid]
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Queries value:
980053277-1733835069-2361817685-1001[profileimagepath]
                   HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
 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]
 Queries value:
 Queries value:
                   HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
HKLM\system\setup[oobeinprogress]
 Oueries value:
 Oueries value:
                   HKLM\system\setup[systemsetupinprogress]
                   HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
 Queries value:
                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                   \label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows}\ nt\current\sc version\sc mage file execution}
 Queries value:
options\dllnxoptions[system.dll]
 Queries value:
11e3-a68e-806e6f6e6963}[data]
 Oueries value:
11e3-a68e-806e6f6e6963}[generation]
 Queries value:
                   HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                   HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Oueries value:
settings[disableimprovedzonecheck]
 Queries value:
                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
                   HKLM\system\currentcontrolset\control\wmi\security[Ocfe0455-93ba-440d-
 Oueries value:
a3fe-553973d0b7231
 Queries value:
                   HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce41
 Oueries value:
                   HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                   HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Queries value:
settings[secureprotocols]
 Queries value:
                   HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                   HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certificaterevocation]
 Queries value:
                   \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[disablekeepalive]
 Queries value:
                   HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                   HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[idnenabled]
 Queries value:
                   HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
 Queries value:
                   HKLM\software\policies\microsoft\windows\currentversion\internet
```

settings[enablehttp1_1]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[proxyhttp1.1]

Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet

settings[proxyhttp1.1]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[proxyhttp1.1]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[enablenegotiate]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[disablebasicoverclearchannel]

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol[feature_clientauthcertfilter]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[clientauthbuiltinui]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[syncmode5]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache[signature]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\content[peruseritem]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [parent folder]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [relative path]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [infotip]$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd\} [icon]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \current \folder \f$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ f9d\} \ [stream resource type]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]

Queries value:

 $\label{local-problem} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\ [roamable]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caedcf9d \ [publish expanded path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ f9d \ [attributes]$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ typeid]$

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]

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

folders[cache]

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-24 fcf-9 d55-7 b8e7 f157091 \cite{thm:local-ham} [category]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parent folder]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [description]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [infotip]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [localized name]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [stream resource type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [local redirectionly]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [roamable]$

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-4fcf-9d55-7b8e7f157091 \[precreate]$

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fits 2785-66 ba-4fcf-9d55-7b8e7f157091 \fits [stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [publish expanded path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[attributes]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} This area wow6432node in crossft windows \end{fiba}. The substitution \end{fiba} This area wow6432node in crossft windows \end{fiba}. This area wow6432node in crossft windows \end{fiba}.$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]

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

folders[local appdata]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cacheprefix]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cachelimit]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[category]}$

Queries value

 $\label{thm:local-condition} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \cdot \cdot \cdot \cdot \folder \cdot \cd$

Queries value:

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [description]$

Queries value

 $\label{local-HKLM} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gray \gray \gray$

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [infotip]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [localized name]$

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [security]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [stream resource]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]$

Queries value:

 $\label{local_ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [precreate]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \cosetware \$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[attributes]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [folder type id]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \ \ coe9-4171-908e-08a611b84ff6 \ [initfolder handler]$

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

folders[cookies]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[cacheprefix]

 $\label{lem:condition} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

settings\5.0\cache\cookies[cachelimit]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [category]$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[relative$ $path]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} [infotip]$

```
b784-432e-a781-5a1130a75963}[localizedname]
 Oueries value:
b784-432e-a781-5a1130a75963}[icon]
 Queries value:
b784-432e-a781-5a1130a75963}[security]
 Oueries value:
b784-432e-a781-5a1130a75963}[streamresource]
 Queries value:
b784-432e-a781-5a1130a75963}[streamresourcetype]
 Queries value:
b784-432e-a781-5a1130a75963}[localredirectonly]
b784-432e-a781-5a1130a75963}[roamable]
 Queries value:
b784-432e-a781-5a1130a75963}[precreate]
b784-432e-a781-5a1130a75963}[stream]
 Queries value:
b784-432e-a781-5a1130a75963}[publishexpandedpath]
b784-432e-a781-5a1130a75963}[attributes]
b784-432e-a781-5a1130a75963}[foldertypeid]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[initfolderhandler]
 Queries value:
                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                  HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cachelimit]
 Oueries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Queries value:
                  \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\domstore[cachepath]
                  HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Oueries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
                  HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                  HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                  HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                  HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                  HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
```

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$

Queries value:

Oueries value:

Queries value:

Queries value:

settings\5.0\cache\extensible cache\ietld[cachepath]

settings\5.0\cache\extensible cache\ietld[cacheprefix]

settings\5.0\cache\extensible cache\ietld[cachelimit]

```
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Oueries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \normalised in the local property of t
  Queries value:
settings[utf8servernameres]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disableworkerthreadhibernation]
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[disableworkerthreadhibernation]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablereadrange]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[socketsendbufferlength]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[socketreceivebufferlength]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperserver]
                                     Queries value:
settings[maxconnectionsperserver]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsper1_0server]
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsper1 Oserver]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[serverinfotimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[receivetimeout]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablentlmpreauth]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[scavengecachelowerbound]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
  Oueries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelimit]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[607c7d18e490c5b56e91c74a29ae3e0a.exe]
```

```
Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Oueries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings[disablecachingofsslpages]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
                          Queries value:
settings[bypasshttpnocachecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                          HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[enablehttptrace]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings[dontusednsloadbalancing]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[mimeexclusionlistforcache]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnalwaysonpost]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpostredirect]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[tcpautotuning]
 Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[winsock registry version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000004 \ [packed catalog item]
```

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 000000000001 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000003 \ [displaystring] \ Oueries \ value:$
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
- 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]
- 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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Queries value:
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ name \ space_catalog \ name \ name \ name \ space_catalog \ name \ n$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 [address family] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]
 Oueries 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\000000000005[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
 Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000006 [address family] \\ Queries \ value:$

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace] \\ Queries value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog \ solves \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
 Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 parameters [ws2_32 numhandle buckets] \\ Queries value: HKCU \software \microsoft \windows \current version \internet \\ HKCU \software \microsoft \windows \current \version \subsection \color="10">10 \symbol{hkl} \symbol{hkl}$

settings\wpad[wpadoverride]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[enableautodial]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[nonetautodial]

settings[globaluseroffline]
 Queries value: HKCU\software\microsoft\windows\currentversion\internet

Queries value: HKL settings[disablebranchcache]

Queries value: HKLM\software\wow6432node\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_http_username_password_disable[607c7d18e490c5b56e91c74a29ae3e0a.exe]|$

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable[*] Queries value: HKLM\software\wow6432node\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_mime_handling[607c7d18e490c5b56e91c74a29ae3e0a.exe]|$

Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[*]

Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
Oueries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enablefiletracing]
 Oueries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[filetracingmask]

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enableconsoletracing] Oueries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[consoletracingmask] Oueries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[maxfilesize]

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[enablefiletracing]
Oueries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[filetracingmask] Oueries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[enableconsoletracing] Queries value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[consoletracingmask]
Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 607 c7 d18e490 c5b56e91c74a29ae3e0a_rasmancs \ [maxfilesize]$

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[filedirectory]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

HKLM\software\microsoft\sqmclient\windows\disabledprocesses[54f8338f] Oueries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]

Queries value: Oueries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]

Oueries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value:

settings[proxysettingsperuser]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[migrateproxy]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings[proxyenable]

HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings[proxyserver]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings[proxyoverride]

 $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ Queries value:

settings[autoconfigurl]

HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings\connections[savedlegacysettings]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\connections[defaultconnectionsettings]

HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]

Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query adapter name]$ Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]

Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$

Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]$

HKLM\svstem\currentcontrolset\services\dnscache\parameters[allowungualifiedguerv]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns secure name query fall back]$

Queries value:

HKLM\svstem\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [queryipm atching]$

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]

HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Queries value: $\label{lem:hklm} \verb+Kklm \system \current control set \services \dns cache \parameters [dnstest]$ Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping] Queries value: ${\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| parameters \verb| winsock [mapping]| \\$ Oueries value: HKLM\svstem\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id] HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] Oueries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6[winsock 2.0 provider id] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [minsock addrlength] \}$

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

Oueries value:

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [search list]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enabled \ hcp]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration enabled]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [register adapter name]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [domain]$

Queries value:

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpdomain]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip6 \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [names erver]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [names erver]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\}[dhcpnameserver]$

Oueries value:

 $\label{thm:local-bound} $HKLM \simeq \sum_{i=1}^{100} \frac{446ee^342-7039-11de-9d^20-806e^66e^6963}{[enabledhcp]} $$ $HCM_{SYS}(0) = \frac{1}{2} \frac{$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [registration enabled]$

Queries value:

 $\label{thm:local-bound} HKLM \system \controlset \services \trpip\parameters \interfaces \end{subseteq} 846ee 342-7039-11 de-9d 20-806e 6f 6e 69 63 \end{subseteq} [register adapter name]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \end{4.846} and \end{4.846$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value: Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [queryadaptername]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [disable adapter domain name]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration maxaddress count]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [maxnumber of addresses to register]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enable multicast]$

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [query adapter name]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [disable adapter domain name]$

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [disable dynamic update]$

Oueries value

 $\label{thm:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable adapter domain name registration]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [registration max address count]$

Queries value:

 $\label{thm:local-bound} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [maxnumber of addresses to register]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable multicast]$

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Oueries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]

Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enablefiletracing] Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enableconsoletracing] Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[filetracingmask]
Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 607 c 7 d 18e 490 c 5b 56e 91 c 74a 29a e 3e 0a_rasapi 32 [consoletracing mask] \\ Sets / Creates value:$

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[maxfilesize]
Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 607 c 7 d 18e 490 c 5b 56e 91 c 74a 29a e 3e 0a_rasapi 32 [filedirectory] \\ Sets \ / Creates \ value:$

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 607 c7 d18e490 c5b56e91c74a29ae3e0a_rasmancs [enable file tracing] \\ Sets \ / Creates \ value:$

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[enableconsoletracing]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[filetracingmask]

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[consoletracingmask]
 Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[maxfilesize]
Sets/Creates value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasmancs [filedirectory]$

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyenable]

 $\label{thm:condition} \begin{tabular}{ll} \b$

 ${\tt settings \backslash connections [savedlegacy settings]}$