Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 214

Task ID: 214 Risk Level: 4

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

Processing Time: 4.96 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]

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

File System Events

Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\</pre>
----------	---

Creates: C:\Users\Admin\AppData\Local\Temp\nsd1279.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nst128A.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nst128B.tmp

Creates: C:\Users
Creates: C:\Users\Admin

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

Creates: C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\System.dll
Creates: C:\Users\Admin\AppData\Local\Temp\nst128B.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\nst128B.tmp\result.txt
Opens: C:\Windows\Prefetch\607C7D18E490C5B56E91C74A29AE3-1B2D8BFB.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe

Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954

 $Opens: C: \verb|Windows| WinSxS| x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\\ \verb|comctl32.dl1|$

```
C:\Windows\SysWOW64\bcryptprimitives.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptbase.dll
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
                         C:\Windows\SysWOW64\oleaut32.dll
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C:\Windows\SysWOW64\shfolder.dll
                         C:\Windows\SysWOW64\SHCore.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
 Opens:
                         C:\Windows\SysWOW64\clbcatq.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\propsys.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db
 Opens:
                         C:\Windows\SysWOW64\desktop.ini
                         C:\Users\Admin\Desktop\desktop.ini
 Opens:
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
                         C:\Windows\SysWOW64\cfgmgr32.dll
 Opens:
                         C:\Windows\SysWOW64\devobj.dll
 Opens:
                         C:\Windows\SysWOW64\setupapi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\nsd1279.tmp
 Opens:
                         C:\Users\Admin\AppData\Local\Temp
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\System.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\zplugins.dll
                         C:\Windows\SysWOW64\iertutil.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C\
 Opens:
                         C:\Windows\SvsWOW64\secur32.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\counters.dat
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winhttp.dll
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc.dll
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
 Opens:
                         C:\Windows\System32\Drivers\etc\hosts
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.DLL
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C
 Opens:
                         C:\Users\Admin\AppData\Local
                         C:\Users\Admin\AppData
 Opens:
                         C:\Users\Admin
 Opens:
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\result.txt
 Writes to:
                         C:\Users\Admin\AppData\Local\Temp\nst128A.tmp
 Writes to:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\System.dll
 Writes to:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\zplugins.dll
 Reads from:
                         C:\Users\Admin\Desktop\desktop.ini
 Reads from:
                         C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe
 Reads from:
                         C:\Users\Admin\AppData\Local\Temp\nst128A.tmp
 Reads from:
                         C:\Windows\System32\Drivers\etc\hosts
 Deletes:
                         C:\Users\Admin\AppData\Local\Temp\nsd1279.tmp
 Deletes:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp
                         Deletes:
 Deletes:
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\System.dll
                         C:\Users\Admin\AppData\Local\Temp\nst128B.tmp\zplugins.dll
```

Network Events

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:	$d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.83$

dl.distromatic.com

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 \Rightarrow 52.73.93.66 DNS response: utrack.n.distromatic.com \Rightarrow 52.87.82.229

Connects to: 54.230.144.39:80
Connects to: 52.73.93.66:80
Sends data to: 0.0.0.0:53

 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: 0.0.0.0:53

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

settings\connections

Creates key: HKLM\system\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]

 $\label{thm:linear} \mbox{Deletes value:} \qquad \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\linear}} \label{thm:linear}$

settings[autodetect]

Opens key: HKLM\software\microsoft\wow64

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

Opens key:

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

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

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

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

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

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

Opens key: HKCU\

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

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

Opens key:

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

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

execution options

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

options\dllnxoptions

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

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

Opens key: HKLM\

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

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

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

Opens key:

 $\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} policies \end{tabular} microsoft \cryptography \configuration$

Opens key: ${\tt HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus ole}$

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

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

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

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

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

Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| policies\\| explorer$

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

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

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

Opens key:

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

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

Opens key: HKCU\software\classes\

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

 $Opens~key: \\ HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04feo-properties} \\ Opens~key: \\ HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04feo-properties} \\ Opens~key: \\$

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

Opens key:

a2d8-08002b30309d}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum

Opens key:

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

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

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

08002b30309d}\inprocserver32

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4c124, d12424, d2424, d$

11e3-be65-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

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

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

Opens key: HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-

97a27216f98a}\inprocserver32

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: $\label{local-opens} \begin{tabular}{ll} HKCU \software \classes \directory \shellex \directory \directory$

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

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

Opens key: HKCR\folder\browseinplace

 $Opens\ key: \\ HKCU \ software \ classes \ all file system objects \ browsein place$

Opens key: HKCR\allfilesystemobjects\browseinplace
Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

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

Opens key: HKCR\folder\clsid

Opens key: ${\tt HKCU \setminus software \setminus classes \setminus all filesystemobjects \setminus clsid}$

Opens key: HKCR\allfilesystemobjects\clsid

Opens key: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-

a6bb2164fbd0}\inprocserver32

Opens key: HKLM\software\microsoft\com3

Opens key: HKLM\software\microsoft\windowsruntime\clsid

 $Opens~key: \\ HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-4g4g4}.$

b8dc300d9f9d}

Opens key: HKCR\activatableclasses\clsid

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

b8dc300d9f9d}

 Opens key:
 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc30d9f9d}

b8dc300d9f9d}\treatas

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key:

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

Opens key:

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db3c,4346,b030,7fe00e97s(41)\renest\rbag

 $db2c-424c-b029-7fe99a87c641\} \setminus property bag$

 $Opens~key: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in fold \\$

Opens key:

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

folders

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ known foldersettings$

Opens key:

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ 1b3ea5dc-b587-4786-b4ef-bd1dc332 aeae \ property bag$

0 ---- l

Opens key

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

Opens key:

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

Opens key

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

Opens kev:

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

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

nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1923240461-1905901954-2556564120-1001

 $Opens\ key: \\ HKLM\software\wow6432 node\microsoft\windows\windows\ error\ reporting\wmr$

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrol\set\control\deviceclasses\{53f5630d-b6bf-11d0-

94f2-00a0c91efb8b}

Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-

94f2-00a0c91efb8b}\properties

Opens key:

11e3-be65-806e6f6e6963}\

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

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

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

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

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

settings\5.0\cache

Opens key:

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

Opens key:

 $\label{thm:local-base-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{352481e8-33be-4251-ba85-6007}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth{\columnwidth}\columnwidth\columnwidth}\columnwidth$

Opens kev: HKU\

Opens key: HKU\.default

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders

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

nt\currentversion\profilelist

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

settings

```
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings
 Opens kev:
                         HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
                         HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol
 Opens kev:
                         HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
                         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
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer \verb|\main| featurecontrol| feature\_fix\_chunked\_proxy\_script\_download\_kb843289
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
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
 Opens key:
                         HKCU\software\microsoft\internet
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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                         HKCU\software\microsoft\internet
 Opens kev:
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
```

HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

Opens key:

```
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_preserve_spaces_in_filenames_kb952730
                     HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
 Opens key:
                     HKCU\software\microsoft\windows\currentversion\internet settings
 Opens key:
                     HKLM\software\wow6432node\policies
 Opens key:
                     HKCU\software\policies
 Opens key:
                     HKCU\software
                     HKLM\software\wow6432node
 Opens key:
 Opens key:
                     HKLM\software\wow6432node\policies\microsoft\internet explorer
 Opens key:
                     HKLM\software\policies\microsoft\internet explorer
 Opens key:
                     HKLM\software\wow6432node\policies\microsoft\internet explorer\main
 Opens key:
                     HKLM\software\policies\microsoft\internet explorer\main
 Opens key:
                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
 Opens key:
                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ 5.0 \ cache
 Opens key:
                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                     HKLM\software\wow6432node\microsoft\internet
 Opens key:
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 key:
                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
                     HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ appid\_catalog \ 00f84a46
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens kev:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
```

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006

HKLM\software\policies\microsoft\peerdist\service Opens kev:

HKLM\software\microsoft\windows nt\currentversion\peerdist\service Opens key:

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

settings\5.0\cache\content

Opens key:

6fba-4fcf-9d55-7b8e7f157091}

Opens key:

6fba-4fcf-9d55-7b8e7f157091}\propertybag

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

settings\5.0\cache\cookies

Opens key:

c0e9-4171-908e-08a611b84ff6}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-164644, 2b0f765d-16464, 2b0f766d-16464, 2b0f766d-16464, 2b0f766d-16464, 2b0f766d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f76d$

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

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

settings\5.0\cache\history

Opens kev:

b784-432e-a781-5a1130a75963}

Opens key:

b784-432e-a781-5a1130a75963}\propertybag Opens kev:

HKLM\system\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

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

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

migration\providers\tcpip6

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

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

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

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

nt\dnsclient\dnspolicyconfig

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

Opens kev:

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

migration\providers\tcpip

 $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient$ Opens key:

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

Opens kev:

 $HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-8$ 55779daa70e9}

Opens key:

806e6f6e6963}

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}

Opens kev:

25b8d56dd1d8}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-

8a6dc56e0da9}

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}

Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage

Opens key:

settings\winhttp

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

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

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

Queries value:

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

Queries value:

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

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

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

us[alternatecodepage]

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

Queries value: $\label{local-control} \begin{tabular}{ll} HKCU \control panel \desktop \muicached [machine preferred uil anguages] \end{tabular}$

Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest] Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo] Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[607c7d18e490c5b56e91c74a29ae3e0a.exe] Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[607c7d18e490c5b56e91c74a29ae3e0a] Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls] HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] ${\tt HKLM \ } software \verb|\ microsoft \ \\ ole[pageallocator system heap is private]$ Oueries value: Queries value: HKLM\software\microsoft\ole[aggressivemtatesting] Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en] Oueries value: Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[attributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[callforattributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[foldervalueflags]

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-

08002b30309d}1

 $HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl$ Oueries value:

08002b30309d}\inprocserver32[]

Queries value:

 $HKCU \ software \ icrosoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c64-7c88-4cq24, d5291c64-7c88-4cq24, d5291c64-7c86-7c88-4cq24, d5291c64-7c86-7c86-7c86-7c$

11e3-be65-806e6f6e6963}[data]

Queries value:

11e3-be65-806e6f6e6963}[generation]

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

409d6c4515e9}[drivemask]

Queries value:

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

HKCU\software\microsoft\windows\currentversion\explorer[shellstate]

Oueries value:

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

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

Queries value:

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

Oueries value:

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

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

Oueries value:

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

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

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

Oueries value:

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

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

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced [filter] \end{tabular}$ Queries value: Oueries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]$ Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar] HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-Queries value: 97a27216f98a}\inprocserver32[] HKCR\directory[docobject] Queries value: Queries value: HKCR\folder[docobject] HKCR\allfilesystemobjects[docobject] Oueries value: Queries value: HKCR\directory[browseinplace] HKCR\folder[browseinplace] Queries value: Queries value: HKCR\allfilesystemobjects[browseinplace] HKCR\directory[isshortcut] Queries value: Queries value: HKCR\folder[isshortcut] Oueries value: HKCR\allfilesystemobjects[isshortcut] HKCR\directory[alwaysshowext] Queries value: HKCR\directory[nevershowext] Oueries value: Queries value: HKCR\folder[nevershowext] HKCR\allfilesystemobjects[nevershowext] Queries value: Queries value: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2ca6bb2164fbd0}\inprocserver32[] HKLM\software\microsoft\com3[com+enabled] Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[] Oueries value: Oueries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32[inprocserver32] HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Queries value: b8dc300d9f9d}\inprocserver32[] HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Queries value: b8dc300d9f9d}\inprocserver32[threadingmodel] Queries value: HKLM\software\microsoft\ole[maxsxshashcount] db2c-424c-b029-7fe99a87c641}[category] HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[name] Oueries value: db2c-424c-b029-7fe99a87c641}[parentfolder] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4$ db2c-424c-b029-7fe99a87c641}[description] Oueries value: db2c-424c-b029-7fe99a87c641}[relativepath] $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4bfcc3a-bc1$ db2c-424c-b029-7fe99a87c641}[parsingname] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[infotip] $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-bc1, b4bfcc3a-bc1, b4bfcc3a-bc1$ db2c-424c-b029-7fe99a87c641}[localizedname] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[icon] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-b$ db2c-424c-b029-7fe99a87c641}[security] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ folder \ descriptions \ folder \ folde$

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

Queries value:

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

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

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{limit} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gam$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[publishexpandedpath]}$

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

folders[desktop]

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Oueries value

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

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:

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

Queries value

Queries value:

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

Queries value:

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

Queries value:

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

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

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Queries value

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [precreate]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdes\cdots\f$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \user shell \end{tabular}$

folders[appdata]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{local-operator} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[relative path]}$

Queries value:

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

Queries value:

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

Oueries value:

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

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

Oueries value:

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

Queries value:

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

Oueries value:

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

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

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

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

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

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

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

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

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \$ 1923240461-1905901954-2556564120-1001[profileimagepath]

Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value: Queries value: $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version [device path]$ $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc file\ execution} \\$ Queries value: options\dllnxoptions[system.dll]

Queries value:

11e3-be65-806e6f6e6963}[data]

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{d5291c63-7c88-4c64, d5291c63-7c88-4c64, d5291c64, d5291c644, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64, d5291c64,$ 11e3-be65-806e6f6e6963}[generation]

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

Oueries value:

Queries value: HKLM\system\setup[oobeinprogress] HKLM\system\setup[systemsetupinprogress] Queries value:

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

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

settings[syncmode5]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

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

Queries value:

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

33be-4251-ba85-6007caedcf9d}[parentfolder]

Queries value:

33be-4251-ba85-6007caedcf9d}[description]

33be-4251-ba85-6007caedcf9d}[relativepath]

Queries value:

33be-4251-ba85-6007caedcf9d}[parsingname]

Oueries value: 33be-4251-ba85-6007caedcf9d}[infotip] Queries value: 33be-4251-ba85-6007caedcf9d}[localizedname] Oueries value: 33be-4251-ba85-6007caedcf9d}[icon] Oueries value: 33be-4251-ba85-6007caedcf9d}[security] Oueries value: 33be-4251-ba85-6007caedcf9d}[streamresource] Oueries value: 33be-4251-ba85-6007caedcf9d}[streamresourcetype] Oueries value: 33be-4251-ba85-6007caedcf9d}[localredirectonly] Queries value: 33be-4251-ba85-6007caedcf9d}[roamable] Queries value: 33be-4251-ba85-6007caedcf9d}[precreate] Queries value: 33be-4251-ba85-6007caedcf9d}[stream] Oueries value: 33be-4251-ba85-6007caedcf9d}[publishexpandedpath] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes] Oueries value: 33be-4251-ba85-6007caedcf9d}[foldertypeid] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (352481e8-16484) \ microsoft \ windows \ current \ version \ (352481e8-16484) \ microsoft \ windows \ current \ version \ (352481e8-16484) \ microsoft \ windows \ current \ version \ (352481e8-16484) \ microsoft \ windows \ current \ version \ (352481e8-16484) \ microsoft \ windows \ (352$ 33be-4251-ba85-6007caedcf9d}[initfolderhandler] HKU\.default\software\microsoft\windows\currentversion\explorer\user Oueries value: shell folders[cache] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[mbcsapiforcrack] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_http_username_password_disable[607c7d18e490c5b56e91c74a29ae3e0a.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_http_username_password_disable[*] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol[feature clientauthcertfilter] HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature mime handling[607c7d18e490c5b56e91c74a29ae3e0a.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[*] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[607c7d18e490c5b56e91c74a29ae3e0a.exe] HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature disable unicode handle closing callback[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[secureprotocols] Oueries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[secureprotocols] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[certificaterevocation]

 $\label{thm:constraint} Queries \ value: \\ \ HKCU\ software\ microsoft\ windows\ current version\ internet \\ settings[preconnectlimit]$

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\windows\currentversion\internet

Queries value:

Queries value:

settings[idnenabled]

settings[disablekeepalive]

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[preresolvelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sqmhttpstreamrandomuploadpoolsize]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cachemode]
 Queries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[clientauthbuiltinui]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enableautoproxyresultcache]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[displayscriptdownloadfailureui]
 Oueries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[utf8servernameres]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
 Queries value:
                          settings[maxconnectionsper1_0server]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperproxy]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certcachenovalidate]
 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[scavengecachefilelifetime]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                           \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}.
  Oueries value:
settings[ftpdefaultexpirytimesecs]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  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[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dialupuselansettings]
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[wpadsearchalldomains]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
                           \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:
settings[bypasssslnocachecheck]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[sharecredswithwinhttp]
                           \label{thm:linear} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
  Queries value:
settings[mimeexclusionlistforcache]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheenabled]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheentries]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonbadcertrecving]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonpostredirect]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonhttpstohttpredirect]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[tcpautotuning]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
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]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries 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\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[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\00000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] 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\0000000000002[displaystring] Oueries 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\000000000002[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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \cat$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000003 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000004 [library path] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [enabled]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 0000000000004 [version]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerinfo]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [displaystring]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[addressfamily]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005[supported name space]]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog5 \ (catalog\_entries \ 000000000006 [library path])
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 \ [address family]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 00000000000006 [version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
  Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets]
                                 HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[proxysettingsperuser]
                                 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
  Queries value:
settings[badproxyexpirestime]
  Queries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[nonetautodial]
  Queries value:
                                 \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[globaluseroffline]
  Queries value:
                                 settings[disablebranchcache]
  Oueries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[combinefalsestartdata]
  Queries value:
                                 HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enforcep3pvalidity]
                                 HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\peerdist\service[enable]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\connections[defaultconnectionsettings]
  Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \ ff 1b 32785-1b 32785-1b
6fba-4fcf-9d55-7b8e7f157091}[category]
  Oueries value:
6fba-4fcf-9d55-7b8e7f157091}[name]
  Oueries value:
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
  Oueries value:
6fba-4fcf-9d55-7b8e7f157091}[description]
  Oueries value:
```

6fba-4fcf-9d55-7b8e7f157091}[relativepath]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{f1b32785-6fba-4fcf-9d55-7b8e7f157091} [folder typeid]$

Queries value:

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

Queries value: folders[local appdata]

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

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{\current} windows \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current \c$

Queries value:

Queries value

 $\label{localized-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescripti$

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\$

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \user shell \end{tabular}$

folders[cookies]

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

settings\5.0\cache\cookies[cachelimit]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \mbox{$d9dc8a3b-b784-432e-a781-5a1130a75963} [description]$

Queries value:

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \mbox{$d9dc8a3b-b784-432e-a781-5a1130a75963} \ [parsing name]$

Queries value:

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

Queries value:

 $\label{thm:localized} HKLM \software \wow 6432 node \mbox{$d9dc8a3b-b784-432e-a781-5a1130a75963} [localized name]$

Queries value:

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

Queries value:

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

```
b784-432e-a781-5a1130a75963}[attributes]
 Oueries value:
b784-432e-a781-5a1130a75963}[foldertypeid]
 Queries value:
b784-432e-a781-5a1130a75963}[initfolderhandler]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                       HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
                       HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [mapping]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                       HKLM\svstem\currentcontrolset\services\winsock\setup
 Oueries value:
migration\providers\tcpip6[winsock 2.0 provider id]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
                       HKU\.default\software\microsoft\windows\currentversion\explorer\user
 Queries value:
shell folders[local appdata]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[migrateproxy]
 Oueries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyserver]
                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[proxyoverride]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[autodetect]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\connections[savedlegacysettings]
 Queries value:
                       HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Queries value:
HKLM \verb| system| current control set \verb| services| dns cache \verb| parameters[used omain name devolution]|
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Queries value:
                       HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
```

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

Queries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [udprecvbuffer size]$ Oueries value: $\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} is supported that the local control of the loc$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries 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] 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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration overwrite]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Queries value: $\label{lem:hklm} \verb+Kklm \system \current control set \services \label{lem:hklm} \verb+ lem \system \current control set \services \label{lem:hklm} \verb+ lem \system \current control set \services \label{lem:hklm} \verb+ lem \system \current control set \system \current \cu$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration] Oueries value:

 $\label{thm:local-control} \parbox{$\tt HKLM} is the {\tt HKLM} system {\tt current} control set {\tt services} {\tt dnscache} {\tt parameters} [newdhcpsrvregistration] \parbox{$\tt extraction} is the {\tt current} control set {\tt current$

Oueries value:

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
 Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
 Oueries value:

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

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

 $\label{thm:local_equation} $$HKLM \simeq \operatorname{Local_ength} = \operatorname{Local_enc} \operatorname{$

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]

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

 $Queries\ value: \\ HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]]$

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip6 \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [search list]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp]

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [registration enabled]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [register adapter name]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled]

Queries value:

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [register adapter name]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain]

Oueries value:

WKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}{nameserver1

Queries value:

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

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \ \finterfaces \ \finterfaces \fin$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ \finterfaces \ \finterfaces \fin$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [registration maxaddress count]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [maxnumber of addresses to register]$

Oueries value

 $\label{lem:hklm} HKLM \ system \ `current controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [enablemulticast]$

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [query adapter name]$

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [disable dynamic update]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [enable adapter domain name registration]$

Oueries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [registration max address count]$

Queries value:

 $\label{thm:local-be} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [maxnumber of addresses to register]$

Queries value:

 $\label{thm:current} Queries \ value: \\ HKLM \ system \ current controls et \ services \ tcpip \ parameters \ [searchlist]$

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

settings[autoproxydetecttype]

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

settings\winhttp[disablebranchcache]

Queries value:

HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]

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

settings[winhttplowercasehost]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdl1] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\history[cacheprefix]

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

settings[proxyenable]

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

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