Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 101, Task ID: 405

Task ID: 405 Risk Level: 1

Date Processed: 2016-04-28 12:57:56 (UTC)

Processing Time: 61.34 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\00aca0729582792a46b971951043ff06.exe"

Sample ID: 101
Type: basic
Owner: admin

Label: 00aca0729582792a46b971951043ff06

Date Added: 2016-04-28 12:45:00 (UTC)

File Type: PE32:win32:gui File Size: 203723 bytes

MD5: 00aca0729582792a46b971951043ff06

SHA256: 0afff2c277d7116b78d29818c8a9422daea4846a70a311c1696f262597209006

Description: None

Pattern Matching Results

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

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\00aca0729582792a46b971951043ff06.exe

["C:\windows\temp\00aca0729582792a46b971951043ff06.exe"]

Named Object Events

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

Creates mutex:

 $\label{local:microsoft:windows:temporary internet} $$ \space{-0.05\textwindows:temporary internet files:content.ie5:} $$ is $$ $$ $$ is $$ is $$ is $$ is $$ is $$ is $$ is $$ is $$ $$ is $$ $$ is $$ is $$ is $$ is $$ $$ is $$ $$ is $$ is $$ $$ is $$$ is $$ $$ is $$ $$ is $$ $$ is $$ $$ is $$$$

'iles!content.ies Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!

Creates mutex:

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

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

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile

Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\BFE_Notify_Event_{81036c73-8a01-4fbe-b702-

55d3e3fe925a}

File System Events

Creates: C:\Users\Admin

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

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files

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

 $\label{lem:condition} Creates: $$C:\Users\landAdmin\landAppData\Roaming\Microsoft\Windows\Cookies$$ Creates: $$C:\Users\landAdmin\landAppData\Local\Microsoft\Windows\History$$$

Creates: C:\Windows\Temp\HandWalletUpdate.original

Opens: C:\Windows\Prefetch\00ACA0729582792A46B971951043F-1D996432.pf

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dl1

 Opens:
 C:\Windows\System32\wow64win.dl1

 Opens:
 C:\Windows\System32\wow64cpu.dl1

 Opens:
 C:\Windows\system32\wow64log.dl1

 Opens:
 C:\Windows\SysWOW64

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

Opens: C:\windows\temp\00aca0729582792a46b971951043ff06.exe.Local\

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

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls 6595b64144ccf1df 6.0.7601.17514 none 41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\SysWOW64\imm32.dll

```
C:\Windows\WindowsShell.Manifest
Opens:
                       C:\windows\temp\00aca0729582792a46b971951043ff06.ENU
Opens:
Opens:
                       C:\windows\temp\00aca0729582792a46b971951043ff06.ENU.DLL
Opens:
                       C:\windows\temp\00aca0729582792a46b971951043ff06.EN
Opens:
                       C:\windows\temp\00aca0729582792a46b971951043ff06.EN.DLL
Opens:
                       C:\Windows\Temp
                       C:\Windows\Temp\00aca0729582792a46b971951043ff06.exe
Opens:
                       C:\Windows\SysWOW64\uxtheme.dll
Opens:
Opens:
                       C:\windows\temp\dwmapi.dll
                       C:\Windows\SysWOW64\dwmapi.dll
Opens:
```

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\windows\temp\HandWalletUpdate.original

Opens: C:\Windows\SysWOW64\http:\www.handwallet.com\update\

Opens: C:\Windows\SysWOW64\wininet.dll
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Local

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\desktop.ini

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\desktop.ini

Opens: C:\Users\Admin\AppData\Roaming

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History

 Opens:
 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini

 Opens:
 C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5

Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\index.dat

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

C:\windows\temp\ntmarta.dll Opens: Opens: C:\Windows\SysWOW64\ntmarta.dll Opens: C:\windows\temp\dnsapi.DLL Opens: C:\Windows\SysWOW64\dnsapi.dll Opens: C:\windows\temp\iphlpapi.DLL Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: C:\windows\temp\WINNSI.DLL Opens: C:\Windows\SysWOW64\winnsi.dll Opens: C:\windows\temp\RASAPI32.dll C:\Windows\SysWOW64\rasapi32.dll Opens: Opens: C:\windows\temp\rasman.dll C:\Windows\SysWOW64\rasman.dll Opens: Opens: C:\windows\temp\rtutils.dll Opens: C:\Windows\SysWOW64\rtutils.dll

Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\

Opens: C:\Windows\SysWOW64\ras

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk

Opens: C:\windows\temp\sensapi.dll
Opens: C:\Windows\SysWOW64\SensApi.dll
Opens: C:\Windows\SysWOW64\nlaapi.dll
Opens: C:\windows\temp\rasadhlp.dll
Opens: C:\Windows\SysWOW64\rasadhlp.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll

Opens: C:\Windows\SysWOW64\en-US\urlmon.dll.mui

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

Opens: C:\Windows\Temp\HandWalletUpdate.original
Opens: C:\windows\temp\HandWalletUpdate.info
Writes to: C:\Windows\Temp\HandWalletUpdate.original

Reads from: C:\Windows\Temp\00aca0729582792a46b971951043ff06.exe

Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from: C:\Windows\Temp\HandWalletUpdate.original

Network Events

DNS query: www.handwallet.com

DNS response: handwallet.com \Rightarrow 198.71.157.117

Connects to: 198.71.157.117:80

Sends data to: 8.8.8.8:53

handwallet.com:80 (198.71.157.117) Sends data to:

Receives data from: 8.8.8.8:53

handwallet.com:80 (198.71.157.117) Receives data from:

Windows Registry Events

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

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

Creates kev:

HKLM\software\wow6432node\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32

Creates kev:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\$ Creates key:

settings\connections

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

 $\label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{$m$icrosoft\windows}$} nt\current version\network\location} \\$ Creates key:

awareness

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

Deletes 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\zonemap[proxybypass]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[intranetname]

 $\label{lem:hklmsoftware} \verb+microsoft+ windows nt+ current version+ image file execution$ Opens key:

options

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

Opens kev: HKLM\software\microsoft\wow64

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

execution options

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

Opens key:

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

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

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

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\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$ Opens key:

Opens key:

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

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

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

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

nt\currentversion\compatibility32

Opens key:

compatibility

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

HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

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

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

HKCU\software\borland\locales Opens key:

Opens key: HKLM\software\wow6432node\borland\locales HKCU\software\borland\delphi\locales Opens key:

Opens key:

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens kev: HKCU\software\pantaray\qsetup\autoupdate Opens key: HKLM\system\currentcontrolset\services\crypt32

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

settings

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings

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

settings

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

settings

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

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

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\policies\microsoft\internet

explorer\main\featurecontrol

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

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

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

explorer\main\featurecontrol

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

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

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

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

Opens key:

Opens key:

 $\label{twarewow6432} HKLM \software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f352481e8-33be-4251-ba85-6007 caedcf9d \end{40}$

Opens key:

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

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

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

Opens key:

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

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

folders

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:

 $\label{twister} HKL\begin{tabular}{l} HKL\$

Opens key:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag$

Opens kev:

 $\label{local-hklm} HKL\begin{tabular}{ll} H$

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-microsoft\} \ description \ folder \$

0e22-4760-9afe-ea3317b67173}\propertybag

 $Opens~key: \\ HKLM \software \wow 6432 node \microsoft \windows \\ nt \current version \profile list \s-1-5-21-980053277-1733835069-2361817685-1001 \\$

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

980053277-1733835069-2361817685-1001

Opens key:

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}

Opens key:

```
c0e9-4171-908e-08a611b84ff6}\propertybag
  Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-microsoft \ wow \ baselines \
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\history
                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\history
  Opens key:
b784-432e-a781-5a1130a75963}
  Opens key:
b784-432e-a781-5a1130a75963}\propertybag
  Opens key:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\domstore
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\extensible cache\feedplat
                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\iecompat
                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\5.0\cache\extensible cache\ietld
                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens kev:
settings\5.0\cache\extensible cache\privacie:
                                  HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                  HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature bufferbreaking 818408
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                  HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
                                  HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key:
                                  \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings\5.0\cache
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                                  HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature disable notify unverified spn kb2385266
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
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
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:
                                  HKCU\software\microsoft\internet
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
                                  HKCU\software\microsoft\internet
  Opens key:
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
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
```

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet$

Opens key:

```
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                   HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                   HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                   HKLM\system\currentcontrolset\control\lsa\accessproviders
 Opens key:
 Opens key:
                   HKLM\system\currentcontrolset\services\ldap
 Opens key:
                   HKLM\system\currentcontrolset\services\winsock2\parameters
                   Opens kev:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1a6fc743
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
                   HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens kev:
 Opens key:
                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                   HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
HKLM\software\wow6432node\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32
 Opens key:
Opens key:
                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
 Opens key:
                   HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
                   HKLM\software\microsoft\sqmclient\windows\disabledsessions\
 Opens kev:
```

HKLM\system\currentcontrolset\control\sqmservicelist

Opens key:

Opens key: HKU\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable
 Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

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

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

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

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

nt\dnsclient\dnspolicyconfig

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

Opens key:

HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig

Opens key: HKCU\software\microsoft\internet

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling

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

explorer\main\featurecontrol\feature_mime_handling

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

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

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key:

settings\zonemap\domains\

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

settings\zonemap\domains

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

settings\zonemap\domains\

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet$

settings\zonemap\ranges\

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

settings\zonemap\ranges

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

settings\zonemap\ranges\

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

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

explorer\main\featurecontrol\feature_unc_savedfilecheck

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

settings\zonemap\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:

 $\label{lem:hklmsoftwarewow6432node} HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet$ Opens key: $\mbox{HKLM\software\policies\microsoft\windows\currentversion\internet}$

settings\zonemap

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

settings\zonemap

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

settings\zonemap\ranges\

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

settings\zonemap\protocoldefaults\

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

settings\zonemap\domains\

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

settings\zonemap\domains\

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

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4

Opens key:

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

settings\zones

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

settings\zones\ Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zones\0

```
Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\1
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
   Opens key:
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\2
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\3
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
   Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\4
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                                 HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                                 HKLM\software\wow6432node\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\
                                                 \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\lockdown_zones
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\0
   Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet
settings\lockdown_zones\0
                                                 \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\lockdown_zones\0
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\0
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\1
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\1
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown zones\2
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown zones\2
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
   Opens key:
                                                 \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\lockdown_zones\3
   Opens key:
settings\lockdown_zones\3
   Opens key:
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens kev:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus micro
settings\lockdown_zones\4
   Opens key:
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
```

```
settings\lockdown_zones\4
                      HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\4
 Opens key:
                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                     HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                      HKCU\software\microsoft\internet explorer\ietld
 Opens key:
                      HKLM\system\currentcontrolset\control\cmf\config
                      HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
 Opens key:
                      HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                      HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
                      HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens kev:
 Opens key:
                      HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                      HKLM\system\currentcontrolset\services\winsock\setup
 Opens key:
migration\providers\tcpip6
 Opens key:
                      HKLM\software\wow6432node\policies\microsoft\system\dnsclient
                      HKLM\software\policies\microsoft\system\dnsclient
 Opens kev:
 Opens key:
                      HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
 Opens key:
e1e01c1f69b5}
 Opens key:
                      HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens kev:
806e6f6e6963}
 Opens kev:
127795cce47a}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
```

65fee5bae0b1}

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

Opens key:

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

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[disableusermodecallbackfilter]

 $\label{thm:current} Queries \ value: \\ HKLM\system\currentcontrolset\control\session$

manager[cwdillegalindllsearch]

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

Queries value:

Queries value:

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

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

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

us[alternatecodepage]

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

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

Queries value:

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

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

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

Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[00aca0729582792a46b971951043ff06]
Oueries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security hklm only] Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440da3fe-553973d0b723] Oueries value: b924-d51178a59ce4] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[secureprotocols] HKCU\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[secureprotocols] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[secureprotocols] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[certificaterevocation] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablekeepalive] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[disablepassport] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[idnenabled] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[enablehttp1_1] HKCU\software\policies\microsoft\windows\currentversion\internet Queries value: settings[enablehttp1_1] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[enablehttp1_1] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[proxyhttp1.1] HKCU\software\policies\microsoft\windows\currentversion\internet Queries value: settings[proxyhttp1.1] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablenegotiate] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[disablebasicoverclearchannel] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol[feature_clientauthcertfilter] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Queries value: HKLM\svstem\currentcontrolset\computername\activecomputername[computername] Queries value: HKLM\system\setup[oobeinprogress] Queries value: HKLM\system\setup[systemsetupinprogress] HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries 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] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\content[peruseritem] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category] HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder] 33be-4251-ba85-6007caedcf9d}[description] Queries value: 33be-4251-ba85-6007caedcf9d}[relativepath] 33be-4251-ba85-6007caedcf9d}[parsingname] Queries value:

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-

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

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

Queries 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:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

folders[cache]

Queries value:

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

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f1b32785-1000\} \\ folder \\ descriptions \setminus \{f1b3275-1000\} \\ folder \\ descriptions \setminus \{f1b3275-10000\} \\ folder \\ descriptions \setminus \{f1b3275-10000\} \\ folder \\ descriptions \setminus \{f1b3275-100000\} \\$ 6fba-4fcf-9d55-7b8e7f157091}[name]

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

Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]

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

Oueries value:

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f 1b32785-b12785 \ \ description \ \ descriptio$ 6fba-4fcf-9d55-7b8e7f157091}[roamable]

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f 1b 32785 - 1b 32785$ 6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]

Queries value:

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

folders[local appdata]

Queries value:

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

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

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

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

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

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

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

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

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ descriptions \setminus \{5e6c858f-microsoft \setminus windows \setminus current \\ descriptions \setminus \{5e6c85microsoft \setminus windows \setminus current \\ descriptions \setminus$ 0e22-4760-9afe-ea3317b67173}[icon]

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

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

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

Oueries value:

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

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

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

Queries value: 980053277-1733835069-2361817685-1001[profileimagepath]

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\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{localized-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe12ed name]$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{\currentversion} explorer \folder descriptions \currentversion \end{\currentversion} explorer \folder descriptions \currentversion \end{\currentversion} explorer \mbox{\currentversion} explorer \mbox{\currentversi$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{limit} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]} \end{tabular}$

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

folders[cookies]

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\calebox{graph}\$

Queries value:

 $\label{local-bound} $HKLM \sim \ensuremath{$\mathbb{C}$ windows \currentversion} \exp \ensuremath{\mathbb{C} a03a-e3ef65729f3d} [name] $$$

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

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

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

folders[appdata]

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

settings\5.0\cache\cookies[cacheprefix]

 $\label{thm:consoft} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\del{hklmsoftware} \del{hklmsoftware} b784-432e-a781-5a1130a75963\folderdescriptions\del{hklmsoftware} \del{hklmsoftware}$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963\}[infotip]}$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3bb784-432e-a781-5a1130a75963\} \ [localized name]$

Queries value:

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

b784-432e-a781-5a1130a75963}[security]

Queries value:

b784-432e-a781-5a1130a75963}[streamresource]

Oueries value:

b784-432e-a781-5a1130a75963}[streamresourcetype]

Oueries value:

b784-432e-a781-5a1130a75963}[localredirectonly]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (d9dc8a3b-descriptions) \ description \ descrip$ b784-432e-a781-5a1130a75963}[roamable]

Oueries value:

b784-432e-a781-5a1130a75963}[precreate]

Oueries value:

b784-432e-a781-5a1130a75963}[stream]

Queries value:

b784-432e-a781-5a1130a75963}[publishexpandedpath]

Oueries value:

b784-432e-a781-5a1130a75963}[attributes]

Queries value:

b784-432e-a781-5a1130a75963}[foldertypeid]

Oueries value:

b784-432e-a781-5a1130a75963}[initfolderhandler]

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

folders[history]

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

settings\5.0\cache\history[cacheprefix]

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

settings\5.0\cache\history[cachelimit]

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

settings\5.0\cache\extensible cache\domstore[cacherepair]

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

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

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

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

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

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

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheoptions]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\feedplat[cacherepair] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

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

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

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

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

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

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

settings\5.0\cache\extensible cache\feedplat[cacheoptions]

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\iecompat[cacherepair]

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

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

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

settings\5.0\cache\extensible cache\iecompat[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

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

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

settings\5.0\cache\extensible cache\iecompat[cacheoptions]

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

settings\5.0\cache\extensible cache\ietld[cacherepair] Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\ietld[cachepath] Queries value:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheprefix]

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

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

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

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

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

settings\5.0\cache\extensible cache\privacie:[cacherepair]

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

settings\5.0\cache\extensible cache\privacie:[cachepath]

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsservername]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsapiforcrack]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[utf8servernameres]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings[maxconnectionsperserver]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
 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[ftpdefaultexpirytimesecs]
 Queries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[00aca0729582792a46b971951043ff06.exe]
                           HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 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[disablecachingofsslpages]
```

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

Queries value:

```
settings[perusercookies]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:
                             HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[dialupuselansettings]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  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[bypasshttpnocachecheck]
                             Oueries value:
settings[bypasshttpnocachecheck]
                             HKCU\software\microsoft\windows\currentversion\internet
  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]
                             \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[dontusednsloadbalancing]
  Queries value:
                             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[sharecredswithwinhttp]
                             \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[mimeexclusionlistforcache]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[headerexclusionlistforcache]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheenabled]
                             \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[dnscacheentries]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscachetimeout]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonzonecrossing]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[warnonbadcertrecving]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[alwaysdrainonredirect]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                             HKLM\system\currentcontrolset\services\ldap[ldapclientintegritv]
  Oueries value:
  Queries value:
                             HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
                             HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Queries value:
  Queries value:
                             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[winsock registry version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 000000000001 \ [packed catalog item]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000003 \ [packed catalog item]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000004 \ [packed catalog item]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]

Queries value:

Queries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerinfo] Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000005 \ [displaystring]$ Oueries value:

Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space _ catalog 5 \ (catalog_entries \ 0000000000005 [supported name space]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled] Queries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000006 \ [displaystring]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[addressfamily] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[version] Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets] Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad[wpadoverride]

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

settings[enableautodial] Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[nonetautodial]

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

settings[globaluseroffline] Oueries value:

HKCU\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime]

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

settings[disablebranchcache]

Queries value: Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 00 aca 0729582792 a 46 b 971951043 ff 06_rasapi 32 [enable file tracing] \ detailed \ file \ file$

HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]

Queries value:

HKLM\software\wow6432node\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[filetracingmask] Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 00 aca 0729582792 a 46 b 971951043 ff 06_rasapi 32 [enable consolet racing]$

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 00 aca 0729582792a46b971951043ff 06_rasapi 32[consoletracing mask]$ Oueries value:

 $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus 00 aca 0729582792a46b971951043ff06_rasapi32[maxfilesize]$ Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 00 aca 0729582792a46b971951043ff 06_rasapi 32[filedirectory]$

HKLM\software\wow6432node\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[enablefiletracing] Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 00aca 0729582792a46b971951043ff 06_rasmancs[filetracing mask]$ Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 00 aca 0729582792 a 46 b 971951043 ff 06_ras mancs \ [enable consolet racing]$

HKLM\software\wow6432node\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[consoletracingmask] Queries value:

 $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus 00 aca 0729582792a46b971951043ff06_rasmancs [maxfilesize]$ Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 00 aca 0729582792a46b971951043ff 06_rasmancs [filedirectory] \ description \ descrip$

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5aa76484]

Queries value:

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

Queries value:

```
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                        HKLM\system\currentcontrolset\control\samservicelist[samservicelist]
 Oueries value:
 Queries value:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[migrateproxy]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyoverride]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[autoconfigurl]
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings\connections[savedlegacysettings]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[defaultconnectionsettings]
                        HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[00aca0729582792a46b971951043ff06.exe]
                        HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[*]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable adapter domain name]
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Queries value:
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[dynamicserverqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                        HKLM\svstem\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration overwrite]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
 Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts endermax time out]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
                        HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_handling[00aca0729582792a46b971951043ff06.exe]
                        HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature mime handling[*]
                        HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[00aca0729582792a46b971951043ff06.exe]
 Queries value:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
                         HKLM\software\policies\microsoft\internet
 Oueries value:
explorer\security[disablesecuritysettingscheck]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\2[flags]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[00aca0729582792a46b971951043ff06.exe]
```

```
Queries value:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Oueries value:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[00aca0729582792a46b971951043ff06.exe]
                       HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Oueries value:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
 Queries value:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[createuricachesize]
 Queries value:
                       HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings[createuricachesize]
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enablepunycode]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablepunycode]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                       HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
 Queries value:
                       HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
 Oueries value:
                       HKLM\svstem\currentcontrolset\control\cmf\config[svstem]
 Queries value:
                       HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
 Queries value:
                       HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\zonemap[autodetect]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[1a10]
                       HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                       HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Queries value:
 Queries value:
                       HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [used elayed acceptance]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
 Queries value:
                       HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
 Queries value:
                       HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                       HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[searchlist]
 Queries value:
e1e01c1f69b5}[enabledhcp]
 Oueries value:
e1e01c1f69b5}[registrationenabled]
 Queries value:
e1e01c1f69b5}[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[domain]
 Oueries value:
e1e01c1f69b5}[dhcpdomain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpv6domain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
 Oueries value:
```

e1e01c1f69b5}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpnameserver] Oueries value: 806e6f6e6963}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled] Oueries value: 806e6f6e6963}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[disableadapterdomainname] e1e01c1f69b5}[registrationmaxaddresscount] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[maxnumberofaddressestoregister] e1e01c1f69b5}[enablemulticast] Queries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername] Oueries value: 806e6f6e6963}[disableadapterdomainname] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate] Oueries value: 806e6f6e6963}[enableadapterdomainnameregistration] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddressestoregister] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value: Oueries value: $HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|$ Sets/Creates value: $HKLM \label{lem:hklm} Software \label{lem:hklm} Wow 6432 node \mbox{\mathbb{Z} node} \mbox{$ Sets/Creates value: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 00 aca 0729582792 a 46 b 971951043 ff 06_rasapi 32 [enable consolet racing] = 0.00 to 100 t$ Sets/Creates value: $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ voaca 0729582792a46b971951043ff 06_rasapi 32[file tracing mask]$ $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus 00aca0729582792a46b971951043ff06_rasapi32[consoletracing mask]$ Sets/Creates value: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 00 aca 0729582792a46b971951043ff06_rasapi32[maxfilesize]$ Sets/Creates value: $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 00 aca 0729582792a46b971951043ff 06_rasapi 32[filedirectory]$

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 00 aca 0729582792 a 46 b 971951043 ff 06_ras mancs [enable file tracing]$

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ voaca 0729582792a46b971951043ff06_rasmancs[file tracing mask]$

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

Sets/Creates value:

Sets/Creates value:

Sets/Creates value:

Sets/Creates value:

 $\label{localize} HKLM software \noise \noi$

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]