## Malware Analysis Appliance by Blue Coat Systems, Inc.

# Task Details

Host: mag2, Sample ID: 619, Task ID: 2423

Task ID: 2423

Risk Level:

Date Processed: 2016-02-22 05:28:19 (UTC)

Processing Time: 61.4 seconds IntelliVM Virtual Environment:

**Execution Arguments:** 

"c:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"

Sample ID: Type: basic Owner:

81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22 Label:

Date Added: 2016-02-22 05:26:49 (UTC)

File Type: PE32:win32:gui File Size: 286720 bytes

MD5: 6f2159e72e7ab7b02e18211ecbed7dd3

SHA256: 81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

Description:

### Pattern Matching Results

1 YARA score 1

6 Modifies registry autorun entries

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

6 Dumps and runs batch script Adds autostart object

4 Terminates process under Windows subfolder

#### Static Events

YARA rule hit: OLE2 YARA rule hit: Nonexecutable

#### Process/Thread Events

C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe ["C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"]

C:\Users\Public\WinJab\winjab.exe ["C:\Users\Public\WinJab\winjab.exe"] Creates process:

Creates process: C:\Windows\system32\cmd.exe [cmd /c C:\Users\Public\1.bat]

Terminates process:

C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe

Terminates process: C:\Windows\System32\cmd.exe

### Named Object Events

Creates mutex \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex:  $\verb|\Sessions|1\BaseNamedObjects| CicLoadWinStaWinStaO|\\$ 

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

 $\verb|\Sessions|1\BaseNamedObjects|_! MSFTHISTORY!_|$ Creates mutex:

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!

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  $\verb|\Sessions|1| BaseNamedObjects| WininetProxyRegistryMutex| \\$ Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1 Creates event: \Sessions\1\BaseNamedObjects\OleDfRootA335511A244DB07D Creates event:

\KernelObjects\MaximumCommitCondition Creates event: Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED \BaseNamedObjects\SvcctrlStartEvent A3752DX Creates event:

\BaseNamedObjects\BFE\_Notify\_Event\_{36dfc21c-93c8-485b-9ebf-Creates event:

9a3c5393a6c3}

Creates event: \BaseNamedObjects\ConsoleEvent-0x00000A28 Creates semaphore: \Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP? 81F686A320DBEC38A90D64C98861F8DDAC8BFDAA7F1AD04A8A33961283E00A22.EXE

\Sessions\1\BaseNamedObjects\C:?USERS?PUBLIC?WINJAB?WINJAB.EXE Creates semaphore:

#### File System Events

Creates: 

C:\Users\Public\WinJab Creates:

Creates: C:\Users\Public\WinJab\winjab.exe

Creates

C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22

C:\Users\Public\1.bat 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 Creates:

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History Creates: C:\Windows\Prefetch\81F686A320DBEC38A90D64C98861F-9845A13B.pf Opens:

C:\Windows\System32 Opens: C:\windows\temp\MSVBVM60.DLL Opens:

```
Opens:
                         C:\Windows\System32\msvbvm60.dll
 Opens:
                         C:\Windows\System32\sechost.dll
 Opens:
                         {\tt C:\Windows\System32\imm32.dll}
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\System32\rpcss.dll
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
 Opens:
                         {\tt C:\Windows\System32\uxtheme.dll}
 Opens:
C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe.cfg
                         C:\windows\temp\SXS.DLL
 Opens:
                         C:\Windows\System32\sxs.dll
 Opens:
                         C:\Windows\System32\C_932.NLS
 Opens:
                         C:\Windows\System32\C_949.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_950.NLS
                         C:\Windows\System32\C_936.NLS
 Opens:
                         C:\windows\temp\winmm.dll
 Opens:
 Opens:
                         C:\Windows\System32\winmm.dll
 Opens:
                         C:\Windows\Fonts\sserife.fon
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
 Opens:
                         C:\Windows\System32\rsaenh.dll
 Opens:
                         C:\windows\temp\dwmapi.dll
 Opens:
                         C:\Windows\System32\dwmapi.dll
 Opens:
                         C:\Windows\Fonts\verdanab.ttf
 Opens:
                         C:\Windows\system32\uxtheme.dll.Config
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
                         C:\Windows\Fonts\lucon.ttf
 Opens:
                         C:\Windows\System32\ieframe.dll
 Opens
 Opens:
                         C:\Windows\System32\oleacc.dll
 Opens:
                         C:\windows\temp\OLEACCRC.DLL
 Opens:
                         C:\Windows\System32\oleaccrc.dll
 Opens:
                         C:\Windows\Fonts\verdana.ttf
 Opens:
                         C:\Windows\System32\asycfilt.dll
 Opens:
                         C:\Windows\System32\winhttp.dll
 Opens:
                         C:\Windows\System32\webio.dll
 Opens:
                         C:\Windows\System32\en-US\KernelBase.dll.mui
 Opens:
                         C:\windows\temp\SspiCli.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\windows\temp\credssp.dll
 Opens:
                         C:\Windows\System32\credssp.dll
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\wshqos.dll
 Opens:
                         C:\windows\temp\wshtcpip.DLL
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\windows\temp\wship6.dll
 Opens:
 Opens:
                         C:\Windows\System32\wship6.dll
                         C:\windows\temp\DNSAPI.dll
 Opens:
 Opens:
                         C:\Windows\System32\dnsapi.dll
 Opens:
                         C:\windows\temp\IPHLPAPI.DLL
                         C:\Windows\Svstem32\IPHLPAPI.DLL
 Opens:
                         C:\windows\temp\WINNSI.DLL
 Opens:
 Opens:
                         C:\Windows\Svstem32\winnsi.dll
                         C:\windows\temp\dhcpcsvc6.DLL
 Opens:
 Opens:
                         C:\Windows\System32\dhcpcsvc6.dll
 Opens:
                         C:\windows\temp\dhcpcsvc.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc.dll
 Opens:
                         C:\windows\temp\rasadhlp.dll
 Opens:
                         C:\Windows\System32\rasadhlp.dll
 Opens:
                         C:\Windows\System32\drivers\etc\hosts
 Opens:
                         C:\Windows\System32\FWPUCLNT.DLL
 Opens:
                         C:\Windows\System32\scrrun.dll
                         C:\Windows\System32\version.dll
 Opens
 Opens:
                         C:\Users\Public\WinJab\
 Opens:
                         C:\Users\Public\WinJab
                         C:\Users\Public\WinJab\winjab.exe
 Opens:
 Opens:
                         C:\Windows\Temp
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
                         C:\Windows\System32\apphelp.dll
                         C:\Windows\AppPatch\sysmain.sdb
 Opens:
 Opens:
                         C:\
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Public
 Opens:
                         C:\Users\Public\WinJab\ui\SwDRM.dll
 Opens:
                         C:\Windows\Prefetch\WINJAB.EXE-59459BCE.pf
 Opens:
                         C:\Users\Public\WinJab\MSVBVM60.DLL
 Opens:
                         C:\Users\Public\WinJab\CRYPTBASE.dll
 Opens:
                         C:\Users\Public\WinJab\winjab.exe.cfg
 Opens:
                         C:\Users\Public\WinJab\SXS.DLL
 Opens:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
 Opens:
                         C:\Users\Public\1.bat
 Opens:
                         C:\windows\temp\cmd.exe
                         C:\Windows\System32\cmd.exe
 Opens:
                         C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
 Opens:
 Opens:
                         C:\Program Files
 Opens:
```

```
Opens:
                          C:\Windows\System32\wininet.dll
 Opens:
                          C:\Program Files\Adobe
                          C:\Program Files\Adobe\Reader 9.0
 Opens:
                          C:\Program Files\Adobe\Reader 9.0\Reader
 Opens:
 Opens:
                          C:\Windows
                          C:\Windows\Branding
 Opens:
                          C:\Windows\Branding\Basebrd
 Opens:
                          {\tt C:\Windows\backslash Branding\backslash Basebrd\backslash en-US}
 Opens:
 Opens:
                          C:\Windows\Globalization
                          C:\Windows\Globalization\Sorting
 Opens:
                          C:\Windows\System32\en-US
 Opens:
                          C:\Windows\System32\ntdll.dll
 Opens:
                          C:\Windows\System32\kernel32.dll
 Opens:
                          C:\Windows\System32\apisetschema.dll
 Opens:
 Opens:
                          C:\Windows\System32\KernelBase.dll
                          C:\Windows\System32\locale.nls
 Opens:
                          C:\Windows\System32\msvcrt.dll
 Opens:
 Opens:
                          C:\Windows\System32\winbrand.dll
 Opens:
                          C:\Windows\System32\user32.dll
 Opens:
                          C:\Windows\System32\gdi32.dll
 Opens:
                          C:\Windows\System32\lpk.dll
 Opens:
                          C:\Windows\System32\usp10.dll
 Opens:
                          C:\Windows\System32\msctf.dll
 Opens:
                          C:\Windows\System32\en-US\cmd.exe.mui
                          C:\Windows\Branding\Basebrd\basebrd.dll
 Opens:
 Opens:
                          C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
                          C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
 Opens:
 Opens:
                          C:\windows\temp\profapi.dll
 Opens:
                          C:\Windows\System32\profapi.dll
                          C:\Users\Admin
 Opens:
                          C:\Users\Admin\AppData\Local
 Opens:
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens
Files\Content.IE5
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\desktop.ini
                          C:\Users\Admin\AppData\Roaming
 Opens:
 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:
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\Content.IE5\index.dat
 Opens:
                          C:\Users\Public\1.bat\
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
\verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\Index.dat| \\
                          C:\windows\temp\ntmarta.dll
 Opens:
 Opens:
                          C:\Windows\Svstem32\ntmarta.dll
                          C:\Windows\WINHELP.INI
 Opens:
 Opens:
                          C:\Windows\system32\.HLP
 Opens:
                          C:\Windows\Help\.HLP
                          C:\Users\Admin\AppData\Local\Temp\~DF220BF13BEA5BF4AC.TMP
 Opens:
                          C:\Users\Public\WinJab\winmm.dll
 Opens:
                          C:\Users\Public\WinJab\winjab.exe
 Writes to:
 Writes to:
                          C:\Users\Public\1.bat
 Reads from:
                          C:\Windows\System32\drivers\etc\hosts
 Reads from:
                          C:\Windows\System32\scrrun.dll
 Reads from:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
  Reads from:
                          C:\Users\Public\WinJab\winjab.exe
 Reads from:
                          C:\Users\Public\1.bat
 Reads from:
                          C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
 Deletes:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
                          C:\Users\Admin\AppData\Local\Temp\~DF220BF13BEA5BF4AC.TMP
 Deletes:
                          C:\Users\Public\1.bat
 Deletes:
Network Events
 DNS query:
                          muzanaczekanie.pl
                          muzanaczekanie.pl ⇒ 188.165.23.155
 DNS response:
                          188.165.23.155:80
 Connects to:
```

Sends data to: 8.8.8.8:53

Sends data to: muzanaczekanie.pl:80 (188.165.23.155) Receives data from: 8.8.8.8:53

muzanaczekanie.pl:80 (188.165.23.155) Receives data from:

#### Windows Registry Events

| Creates key:   | HKLM\system\currentcontrolset\services\tcpip\parameters                     |
|----------------|---|
| Creates key:   | HKCU\software\microsoft\windows\currentversion\run                          |
| Creates key:   | HKCU\software\vb and vba program settings\clock\sdata                       |
| Creates key:   | HKCU\software   |
| Creates key:   | HKCU\software\vb and vba program settings                                   |
| Creates key:   | HKCU\software\vb and vba program settings\clock                             |
| Creates key:   | <pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre> |
| Deletes value: | HKCII\software\microsoft\internet   |

```
explorer\lowregistry[addtofavoritesinitialselection]
      Deletes value:
                                                                                         HKCU\software\microsoft\internet
 explorer\lowregistry[addtofeedsinitialselection]
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\session manager
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\terminal server
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\safeboot\option
                                                                                         HKLM\system\currentcontrolset\control\srp\gp\dll
      Opens key:
                                                                                         \label{lem:hklmsoftware policies microsoft windows safer code identifiers \\
      Opens key:
      Opens kev:
                                                                                         \label{lem:hkcu} \verb+KCU\+software\+policies\+microsoft\+windows\+safer\+codeidentifiers
      Opens kev:
                                                                                         HKCU\
                                                                                         HKCU\control panel\desktop\muicached\machinelanguageconfiguration
      Opens key:
      Opens key:
                                                                                         HKLM\software\policies\microsoft\mui\settings
                                                                                         HKCU\software\policies\microsoft\control panel\desktop
      Opens key:
      Opens kev:
                                                                                         HKCU\control panel\desktop\languageconfiguration
      Opens key:
                                                                                         HKCU\control panel\desktop
                                                                                         HKCU\control panel\desktop\muicached
      Opens kev:
                                                                                         HKLM\software\microsoft\windows\currentversion\sidebyside
      Opens kev:
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\nls\sorting\versions
     Opens key:
                                                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options
     Opens key:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\error message instrument\
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\error message instrument
      Opens key:
                                                                                         HKLM\software\microsoft\windows nt\currentversion\gre_initialize
      Opens key:
                                                                                         HKLM\software\microsoft\windows nt\currentversion\compatibility32
      Opens key:
                                                                                         HKLM\software\microsoft\windows nt\currentversion\ime compatibility
      Opens key:
                                                                                         HKLM\
      Opens key:
                                                                                         HKLM\software\microsoft\windows nt\currentversion\windows
                                                                                         \label{thm:local_hammon} \mbox{HKLM} \mbox{$\tt MKLM} \mbox{$\tt MKL
      Opens key:
      Opens key:
                                                                                         HKLM\software\microsoft\ole
      Opens key:
                                                                                         HKLM\software\microsoft\ole\tracing
      Opens key:
                                                                                         HKLM\software\microsoft\oleaut
      Opens key:
                                                                                         HKLM \verb|\system| current controlset \verb|\control| nls \verb|\custom| locale
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\nls\extendedlocale
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\nls\locale
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\nls\language groups
      Opens key:
                                                                                         HKLM\software\microsoft\windows\windows error reporting\wmr
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\nls\codepage
      Opens key:
                                                                                         HKLM\software\microsoft\vba\monitors
      Opens key:
HKLM \setminus software \\ \setminus compatibility \setminus 81f686a320 \\ dbec38a90 \\ d64c98861f8 \\ ddac8bf \\ daa7f1ad04a8a33961283e00a22. \\ exemple \\ exemple \\ \Delta P = 1000 \\ \Delta P = 1000
      Opens key:
                                                                                         HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be18 - b
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
      Opens key:
                                                                                         HKLM\software\microsoft\ctf\
                                                                                         HKLM\software\microsoft\ctf\knownclasses
      Opens kev:
      Opens key:
                                                                                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong
cryptographic provider
                                                                                         HKLM \verb|\system| current controlset \verb|\control| lsa \verb|\fipsalgorithm| fipsalgorithm| final substitution for the substitution of the substitution 
      Opens key:
                                                                                         HKLM\system\currentcontrolset\control\lsa
      Opens key:
      Opens kev:
\label{thm:linear} \begin{tabular}{ll} HKLM \end{tabular} is system \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} system \end{tabular} \begin{tabular}{ll} constraints \end{tabular} is system \end{tabular} \begin{tabular}{ll} constraints \end{t
      Opens kev:
                                                                                         HKLM\software\policies\microsoft\cryptography
      Opens key:
                                                                                         HKLM\software\microsoft\cryptography
      Opens key:
                                                                                         HKLM\software\microsoft\cryptography\offload
      Opens kev:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
                                                                                         HKCU\software\classes\
      Opens kev:
      Opens key:
                                                                                         HKLM\software\microsoft\com3
                                                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
      Opens key:
      Opens key:
                                                                                         HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
     Opens key:
                                                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
 00c04fd705a2}\treatas
                                                                                         HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
      Opens key:
      Opens key:
                                                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
 00c04fd705a2}\progid
      Opens key:
                                                                                          HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
                                                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
      Opens key
00c04fd705a2}\inprocserver32
                                                                                         Opens key:
                                                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
       Opens key:
00c04fd705a2}\inprochandler32
                                                                                         HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
      Opens kev:
                                                                                         HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b
      Opens key:
00c04fd705a2}\inprochandler
                                                                                         Opens key:
      Opens key:
                                                                                         HKLM\software\microsoft\rpc
      Opens key:
                                                                                         \label{thm:local_transform} \begin{tabular}{ll} HKLM \end{tabular} system \current control \computer name \end{tabular} active computer name \end{tabular} active computer name \end{tabular} active \computer n
                                                                                         HKLM\system\setup
      Opens key:
      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:
                                                                                         HKCU\software\classes\clsid\{00021401-0000-0000-c000-00000000046}
      Opens key:
                                                                                         HKCR\clsid\{00021401-0000-0000-c000-00000000046}
                                                                                         HKCU\software\classes\clsid\{00021401-0000-0000-c000-
      Opens key:
000000000046}\treatas
      Opens key:
                                                                                         HKCR\clsid\{00021401-0000-0000-c000-00000000046}\treatas
      Opens key:
                                                                                         HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\progid
                                                                                          HKCR\clsid\{00021401-0000-0000-c000-00000000046}\progid
      Opens key:
                                                                                         HKCU\software\classes\clsid\{00021401-0000-0000-c000-
      Opens key:
000000000046}\inprocserver32
```

HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32

Opens key:

```
Opens key:
                             HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:
                             HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandler32
  Opens key:
                             HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandler
  Opens key:
                             HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandler
  Opens key:
                             HKLM\system\currentcontrolset\services\crypt32
  Opens key:
                             HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key:
                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings
                             HKLM\software\microsoft\oleaut\userera
 Opens key:
  Opens key:
                             HKCU\software\policies\microsoft\control
panel\international\calendars\twodigityearmax
                             HKCU\control panel\international\calendars\twodigityearmax
  Opens kev:
                             HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}
  Opens key:
                             HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}
  Opens kev:
  Opens kev:
                             HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\treatas
                             HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\treatas
  Opens key:
                             HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
  Opens key:
66779b670495}\progid
                             HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\progid
  Opens key:
 Opens kev:
                            HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32
  Opens key:
                            HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserver32
                             HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
  Opens key:
66779b670495}\inprochandler32
  Opens key:
                             HKCR \verb|\clsid|{2087c2f4-2cef-4953-a8ab-66779b670495} \verb|\inprochandler32|
  Opens key:
                             HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprochandler
  Opens kev:
                             HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandler
  Opens key:
                             HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:
                             HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
  Opens key:
                             HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
                             HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\07a0e1d6
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries
  Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ possible \ and \ protocol\_catalog \ protocol\_catal
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000
  Opens key:
Opens kev:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
 Opens key:
Opens kev:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ 0000000000013
  Opens key:
Opens kev:
Opens key:
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 0000000000017
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003

Opens key:

Opens key:

```
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
 Opens key:
                       HKLM\system\currentcontrolset\control\cmf\config
 Opens key:
                       HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
 Opens key:
                       HKLM\system\currentcontrolset\control\securityproviders
 Opens key:
                       HKLM\system\currentcontrolset\control\lsa\sspicache
 Opens key:
                       HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
                       HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
 Opens kev:
                       HKLM\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\connections
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
                       HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
                       HKLM\system\currentcontrolset\services\psched\parameters\winsock
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens kev:
                       HKLM\system\currentcontrolset\services\winsock\setup
 Opens kev:
migration\providers\psched
 Opens kev:
                       HKLM\system\currentcontrolset\services\dnscache\parameters
```

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

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

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

Opens key:

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

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

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

migration\providers\tcpip

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

migration\providers\tcpip6

Opens key: HKLM\software\policies\microsoft\system\dnsclient HKLM\system\currentcontrolset\control\sqmservicelist Opens kev:

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

Opens key:

c19ce8a73253}

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}

Opens key:

806e6f6e6963} Opens key:

806e6f6e6963} Opens kev:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-

1709a0196aed3

Opens key: 

a68f334c8d34}

HKLM\svstem\currentcontrolset\services\tcpip\linkage Opens kev:

Opens kev:  ${\tt HKCU \backslash software \backslash classes \backslash scripting.filesystemobject}$ 

Opens key: HKCR\scripting.filesystemobject

Opens key:  ${\tt HKCU \setminus software \setminus classes \setminus scripting.filesystemobject \setminus clsid}$ 

HKCR\scripting.filesystemobject\clsid Opens key:

HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228} Opens kev:

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228} Opens key: Opens kev: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\treatas

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\progid

Opens key: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\progid Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32

Opens key: HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32

Opens key: HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprochandler32

HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler32 Opens key:

HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-Opens key:

00a0c9054228}\inprochandler

 $HKCR \ clsid \ \{0d43fe01-f093-11cf-8940-00a0c9054228\} \ \ in prochandler$ Opens key:

Opens kev: HKCU\software\classes\tvpelib

Opens key: HKCR\typelib

Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}

Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0 Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-

00a0c9054228}\1.0\0

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0 Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-

00a0c9054228}\1.0\0\win32

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32

Opens key: HKCU\software\vb and vba program settings\clock\sdata

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

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

options\winjab.exe

HKLM\svstem\currentcontrolset\control\session manager\appcertdlls Opens kev: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key:

```
Opens key:
                                                                                     HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
      Opens key:
                                                                                     HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\winjab.exe
      Opens key:
                                                                                    HKLM\software\microsoft\windows
 nt\currentversion\appcompatflags\custom\1.bat
      Opens key:
                                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
     Opens key:
                                                                                     HKCU\software\policies\microsoft\windows\currentversion\internet
 settings
      Opens kev:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet settings
                                                                                     HKLM\software\policies
      Opens key:
                                                                                     HKCU\software\policies
      Opens key:
      Opens key:
                                                                                     HKCU\software
      Opens key:
                                                                                     HKLM\software
      Opens key:
                                                                                     HKLM\software\policies\microsoft\internet explorer
      Opens kev:
                                                                                     HKLM\software\policies\microsoft\internet explorer\main
                                                                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$\operatorname{HKLM} \end{tabular} in \begin{tabular}{ll} \dot{\end{tabular}} in \begin{tabular}{ll} \dot{\end
      Opens kev:
      Opens kev:
                                                                                     HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
      Opens kev:
                                                                                     \label{thm:hkcu} \begin{tabular}{ll} HKCU\software\mbox{$\stackrel{\cdot}{m}$ icrosoft\internet explorer\mbox{$\stackrel{\cdot}{m}$ in\end{tabular} } \\ \end{tabular}
      Opens key:
                                                                                     \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ internet explorer \+ main \+ feature control
     Opens key:
                                                                                     HKLM\software\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:
                                                                                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\content
      Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions
      Opens kev:
ba85-6007caedcf9d}
      Opens key:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Which is a simple of the latest and the latest angle of the latest and the latest and the latest angle of the latest angle 
ba85-6007caedcf9d}\propertybag
      Opens key:
                                                                                     HKCU\software\microsoft\windows\currentversion\explorer
                                                                                     HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in fo \setminus 1
      Opens key:
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders
                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Opens key:
 folders
      Opens key:
                                                                                     HKLM\software\policies\microsoft\windows\explorer
      Opens key:
                                                                                     HKCU\software\policies\microsoft\windows\explorer
      Opens key:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \l
9d55-7b8e7f157091}
      Opens key:
9d55-7b8e7f157091}\propertybag
      Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
                                                                                     HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
      Opens key
2160590473-689474908-1361669368-1002
     Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                                                    HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
settings\5.0\cache\cookies
                                                                                    HKLM\software\microsoft\windows\currentversion\internet
    Opens key:
settings\5.0\cache\cookies
      Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-descriptions\} \ for the software \ microsoft \ windows \ not the software \ microsoft \ microso
908e-08a611b84ff6}
     Opens key:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `explore
908e-08a611b84ff6}\propertybag
      Opens key:
a03a-e3ef65729f3d}
      Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
      Opens key
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                                                                                     HKLM\software\microsoft\windows\currentversion\internet
     Opens key:
 settings\5.0\cache\history
a781-5a1130a75963}
      Opens key:
a781-5a1130a75963}\propertybag
      Opens key:
                                                                                     HKCU\software\policies\microsoft\windows\system
      Opens key:
                                                                                     HKLM\software\microsoft\command processor
```

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones

HKCU\software\microsoft\command processor

HKLM\software\policies\microsoft\windows\safer\levelobjects

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths

 $\label{thm:local_hammon} HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes$ 

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

```
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
   Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
   Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 131072 \ paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
   Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
   Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
                                                 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
   Opens key:
   Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \parbox{0.4mm} \code id
   Opens key:
HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ paths
   Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
    Opens key:
Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus has hes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
   Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
   Opens key:
\label{thm:local-obs} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \code \code\
   Opens key:
                                                 HKLM\system\currentcontrolset\control\srp\\gp\
                                                 HKLM\svstem\currentcontrolset\control\srp\\gp
   Opens key:
   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 kev:
settings\5.0\cache\extensible cache\iecompat
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\extensible cache\ietld
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\extensible cache\privacie:
   Opens key:
                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
   Opens key:
                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
   Opens kev:
                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature bufferbreaking 818408
   Opens key:
                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache
   Opens key:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
   Opens key:
                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
   Opens key:
                                                 HKLM\software\microsoft\internet
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\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\microsoft\internet
```

 $explorer \verb|\main| feature a ture_disable_notify_unverified\_spn\_kb2385266$ 

```
Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                          HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_allow_long_international\_file names|\\
 Opens key:
                          HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names|\\
 Opens key:
                          HKCU\software\microsoft\internet
\verb|explorer| wain feature control feature permit_cache for authenticated ftp\_kb910274| \\
 Opens kev:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens kev:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens kev:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens kev:
                          HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_use\_utf8\_for\_basic\_auth\_kb967545
                          HKLM\software\microsoft\internet
 Opens key:
explorer \verb|\main| featurecontrol| feature\_use\_utf8\_for\_basic\_auth\_kb967545
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                          HKLM \setminus system \setminus current control \setminus lsa \setminus access providers
 Opens key:
                          HKLM\system\currentcontrolset\services\ldap
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\cache
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\cache
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\cache
 Opens key:
                          \label{prop:lower} \verb+HKCU\+ software\+ microsoft\+ internet explorer\+ low registry
                          HKLM\software\microsoft\windows
 Opens key:
                          HKLM\software\microsoft\windows\html help
 Opens kev:
                          HKLM\software\microsoft\windows\help
 Opens key:
                          HKLM\system\currentcontrolset\control\session
 Oueries value:
manager[cwdillegalindllsearch]
                          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value:
                          HKCU\control panel\desktop[preferreduilanguages]
 Oueries value:
                          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Oueries value:
HKLM \verb|\software\microsoft\windows\currentversion\side| preferexternal manifest| \\
                          HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                          \label{thm:local_hammon} \mbox{HKLM} \mbox{`software} \mbox{`microsoft} \mbox{`windows nt} \mbox{`currentversion} \mbox{`image file execution}
 Oueries value:
options\dllnxoptions[msvbvm60.dll]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                          HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
 Queries value:
                          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Oueries value:
                          {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocator system heap is private]}
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:
                          \label{lem:hklmsystem} \\ \text{HKLM} \\ \text{System} \\ \text{control} \\ \text{nls} \\ \text{extendedlocale[en-us]} \\
 Queries value:
                          Queries value:
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                          HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
 Oueries value:
                          {\it HKLM} \verb|\system| current controlset| control \verb|\session| \\
manager[safeprocesssearchmode]
                          HKLM\svstem\currentcontrolset\control\nls\codepage[932]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\control\nls\codepage[949]
                          HKLM\system\currentcontrolset\control\nls\codepage[950]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\control\nls\codepage[936]
```

HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-

Oueries value:

```
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
                  HKLM\software\microsoft\ctf[enableanchorcontext]
 Oueries value:
 Queries value:
                  \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong
cryptographic provider[type]
 Queries value:
                  \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong
cryptographic provider[image path]
 Queries value:
                  HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Queries value:
                  {\tt HKLM \ } system \verb|\ current control \ \\ lsa[fips algorithm policy]
 Oueries value:
                  \label{locality} \verb|HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]| \\
 Oueries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                  HKLM \verb|\software\policies\m| icrosoft \verb|\cryptography[privatekeylifetimeseconds]| \\
 Queries value:
                  {\tt HKLM \coftware \microsoft \cryptography[machineguid]}
 Oueries value:
                  HKLM\software\microsoft\com3[com+enabled]
 Oueries value:
                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
 Oueries value:
                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
 Oueries value:
                  HKCR\clsid\{8856f961-340a-11d0-a96b-
 Oueries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
 Oueries value:
                  HKCR\clsid\{8856f961-340a-11d0-a96b-
 Queries value:
00c04fd705a2}\inprocserver32[threadingmodel]
                  HKLM\software\microsoft\ole[maxsxshashcount]
 Queries value:
 Oueries value:
                  HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
Queries value:
                  HKLM\system\setup[oobeinprogress]
 Queries value:
                  HKLM\system\setup[systemsetupinprogress]
 Queries value:
                  HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
                  HKCR\clsid\{00021401-0000-0000-c000-00000000046}\progid[]
 Oueries value:
                  HKCR\clsid\{00021401-0000-0000-c000-00000000046}[]
 Oueries value:
                  HKCR\clsid\{00021401-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                  HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32[]
 Queries value:
                  HKCR\clsid\{00021401-0000-0000-c000-
 Queries value:
00000000046}\inprocserver32[threadingmodel]
 Queries value:
                  HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                  HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableimprovedzonecheck]
                  \label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ windows \+ current \+ version \+ internet
 Queries value:
settings[security_hklm_only]
                  HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\progid[]
 Queries value:
 Queries value:
                  HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}[]
 Queries value:
                  HKCR\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32[inprocserver32]
 Queries value:
                  HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserver32[]
 Oueries value:
                  HKCR\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32[threadingmodel]
 Queries value:
                  HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing[enabled]
 Queries value:
                  HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Oueries value:
                  HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog9[serial\_access\_num]
 Oueries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9[next catalog entry id]
 Queries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ octalog\_entries \ 000000000001 \ [packed catalog item]
 Queries value:
Oueries value:
Queries value:
Queries value:
Oueries value:
Queries value:
Queries value:
Queries value:
Queries value:
Queries value:
Oueries value:
Oueries value:
Queries value:
Queries value:
```

```
HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ \ 0000000000016 \ [packed catalog item] \ Queries \ value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000017[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000018[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
Oueries value:

 $HKLM\system\current control set\services\winsock 2\parameters\namespace\_catalog 5\catalog\_entries\00000000001[library path]\\ Queries\value:$ 

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \noon 00000000001 \[displaystring]\queries \value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$ 

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \000000000001 \[storesservice class in fo] \queries value:$ 

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names \nam$ 

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \000000000000002 \[displaystring]\queries \value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[supportednamespace] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerid] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]

 $\label{lem:parameters} Queries \ value: $$HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[supported namespace]$$$ 

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[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] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo] Oueries value:

 $\label{thm:local-parameters} HKL^{M} system \verb|\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\\ Catalog\_entries\\ 000000000000004[displaystring] \\ Queries value:$ 

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \000000000000004 \[address family]\] Queries value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace]
Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
 Oueries value:

 $HKLM\system\current control set\services\winsock 2\parameters\namespace\_catalog 5\catalog\_entries\000000000004[storesserviceclassinfo]\queries\value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo] Oueries value:

 $\label{limits} \begin{tabular}{ll} HKLM system \verb|currentcontrolset|services|winsock2|parameters|namespace_catalog5|catalog_entries|00000000005[librarypath]| Queries value: \end{tabular}$ 

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \noon 00000000005 \[address family]\] Queries value:$ 

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \noon00000000005 \[supported namespace\_Queries \value: \] \\$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled] Oueries value:

```
HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ catalog\_entries \ \ \ 000000000005 \ [version]
  Oueries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 00000000005 \ [storesserviceclassinfo]
  Oueries value:
Oueries value:
HKLM \ system \ current control set \ services \ win sock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 0000000000006 [library path]
  Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\000000000006[providerid]
  Queries value:
Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006fenabled1
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[version]
  Queries value:
HKLM \ system \ catalog 5 \ catalog\_entries \ 000000000006 [storesservice class in fo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:
                                 HKLM\system\currentcontrolset\config[system]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
  Oueries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
HKLM \setminus system \setminus current control \setminus security providers [security providers]
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Queries value:
  Queries value:
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Queries value:
  Oueries value:
                                 HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Queries value:
                                 HKLM \setminus system \setminus current control \\ \  \mid sa \setminus spicache \setminus credssp. \\ dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Oueries value:
                                 HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
  Oueries value:
                                 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
  Queries value:
                                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
  Oueries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[maxsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[usedelayedacceptance]
  Oueries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[helperdllname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
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]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [append to multilabel name]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
\label{lem:hklm} \verb+Kklm \system \current control set \services \
  Queries value:
\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+dns \ cache \ \verb+parameters \ [screen default servers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
```

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

Oueries value:

Oueries value:

```
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns secure name query fall back]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
  Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Oueries value:
                                     HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[use hostsfile]|
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration enabled]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Oueries value:
\label{thm:local_control} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \color= control set \end{tabular} and \color= control set \end{tabular} set \color= control s
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Oueries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [register reverse lookup]
  Oueries value:
HKLM \label{likelihood} System \current control set \scrvices \tcpip \parameters [disable reverse address registrations]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [updates ecurity level]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]
  Oueries value:
Queries value:
HKLM \verb|\system| current control set \verb|\services| dns cache \verb|\parameters| [max cache size]|
  Oueries value:
  Oueries value:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Oueries value:
Oueries value:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [resolver registration]
  Queries value:
\label{lem:hklm} \verb+Kklm/system/currentcontrolset/services/dnscache/parameters[resolverregistrationonly]+ \\
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns quick query time outs]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]
  Queries value:
                                     \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ tcpip \+ parameters \+ winsock \+ [mapping]
  Oueries value:
                                     HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
```

Oueries value:

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

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [helperdllname]$ 

Queries value:  ${\tt HKLM \ } system \verb| current control set \verb| services \verb| winsock \verb| setup | \\$ migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonid]el

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[searchlist]

Oueries value:

c19ce8a73253}[enabledhcp]

Queries value:

c19ce8a73253}[registrationenabled]

Queries value:

c19ce8a73253}[registeradaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[domain]

Queries value:

c19ce8a73253}[dhcpdomain]

Queries value:

c19ce8a73253}[dhcpv6domain]

Queries value:

c19ce8a73253}[nameserver]

Queries value:

c19ce8a73253}[nameserver]

Oueries value:

c19ce8a73253}[dhcpnameserver]

Queries value:

806e6f6e6963}[enabledhcp]

Oueries value:

806e6f6e6963}[registrationenabled]

Oueries value:

 $\label{local-control} HKLM \xspace \$ 806e6f6e6963}[registeradaptername] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpdomain]

Oueries value:

806e6f6e6963}[nameserver]

Queries value:

806e6f6e6963}[dhcpnameserver]

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

Queries value:

c19ce8a73253}[queryadaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[disableadapterdomainname]

Queries value:

c19ce8a73253}[registrationmaxaddresscount]

Oueries value:

c19ce8a73253}[maxnumberofaddressestoregister]

Queries value:

c19ce8a73253}[enablemulticast]

Queries value:

806e6f6e6963}[queryadaptername]

Oueries value:

806e6f6e6963}[disableadapterdomainname]

Oueries value:

```
806e6f6e6963}[disabledynamicupdate]
 Oueries value:
{\tt 806e6f6e6963} [enable adapter domain name registration]\\
 Queries value:
806e6f6e6963}[registrationmaxaddresscount]
 Oueries value:
806e6f6e6963}[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enablemulticast]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Oueries value:
                         HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Oueries value:
                         HKCR\scripting.filesystemobject\clsid[]
 Oueries value:
                         HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\progid[]
 Oueries value:
                         HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]
 Oueries value:
                         HKCR\clsid\{0d43fe01-f093-11cf-8940-
 Oueries value:
00a0c9054228}\inprocserver32[inprocserver32]
                         HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{0d43fe01-f093-11cf-8940-
 Queries value:
00a0c9054228}\inprocserver32[threadingmodel1
                         HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]
 Queries value:
 Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
 Queries value:
                         HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
 Queries value:
                         HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
  Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\users\public\winjab\winjab.exe]
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[winjab]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\appcompatflags\layers[c:\users\public\1.bat]
                         Queries value:
a3fe-553973d0b723]
 Queries value:
                         \label{lem:hklm} \verb+Kklm \ system \ current control \ \verb+vemi \ security [797 fabac - 7b58 - 4796 - 4796 - 4796] \\
b924-d51178a59ce41
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
 Queries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
 Queries value:
                         \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[secureprotocols]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certificaterevocation]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablepassport]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[idnenabled]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cachemode]
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1 1]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Oueries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                         \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[proxyhttp1.1]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value
                         HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
                         HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
                         \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
 Queries value:
settings[syncmode5]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
{\tt settings \ 1.0 \ cache[sessionstart time default delta secs]}
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\internet
```

settings\5.0\cache\content[peruseritem]

Oueries value:

ba85-6007caedcf9d}[category]

Queries value:

ba85-6007caedcf9d}[name]

Queries value:

ba85-6007caedcf9d}[parentfolder]

Oueries value:

 $HKLM \label{lem:hkk} In the latest and the latest$ ba85-6007caedcf9d}[description]

Oueries value:

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

Oueries value:

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

Oueries value:

ba85-6007caedcf9d}[infotip]

Queries value:

ba85-6007caedcf9d}[localizedname]

Queries value:

ba85-6007caedcf9d}[icon]

Queries value:

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

Oueries value:

ba85-6007caedcf9d}[streamresource]

ba85-6007caedcf9d}[streamresourcetype]

ba85-6007caedcf9d}[localredirectonly]

Oueries value:

ba85-6007caedcf9d}[roamable]

Queries value:

ba85-6007caedcf9d}[precreate]

Oueries value:

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

Queries value:

ba85-6007caedcf9d}[publishexpandedpath] Oueries value:

ba85-6007caedcf9d}[attributes] Oueries value:

ba85-6007caedcf9d}[foldertypeid] Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-

ba85-6007caedcf9d}[initfolderhandler]

Oueries value: folders[cache] HKCU\software\microsoft\windows\currentversion\explorer\user shell

Queries value:

9d55-7b8e7f157091}[category]

Queries value:

 $HKLM \label{lem:hkkkk} Which is the software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fill derdescriptions| folder descriptions $|\fill derdes$ 9d55-7b8e7f157091}[name]

9d55-7b8e7f157091}[parentfolder]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ expl$ 9d55-7b8e7f157091}[description]

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-1000' \ explorer \ 'folder descriptions' \ 'f1b32785-6fba-4fcf-1000' \ explorer \ explorer \ 'f1b32785-6fba-4fcf-1000' \ explorer \ expl$ 9d55-7b8e7f157091}[relativepath]

9d55-7b8e7f157091}[parsingname]

Oueries value:

9d55-7b8e7f157091}[infotip]

Queries value:

9d55-7b8e7f157091}[localizedname]

Queries value:

9d55-7b8e7f157091}[icon]

Oueries value:

9d55-7b8e7f157091}[security]

Oueries value:

9d55-7b8e7f157091}[streamresource]

Oueries value:

9d55-7b8e7f157091}[streamresourcetype]

Queries value:

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

Oueries value:

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

Oueries value:

9d55-7b8e7f157091}[precreate]

Oueries value:

9d55-7b8e7f157091}[stream]

Oueries value:

9d55-7b8e7f157091}[publishexpandedpath]

Queries value:

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

Oueries value:

 $HKLM \label{lem:hkkkk} Which is the software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\fill derdescriptions| folder descriptions $|\fill derdes$ 9d55-7b8e7f157091}[foldertypeid]

Oueries value:

9d55-7b8e7f157091}[initfolderhandler]

folders[local appdata]

Queries value:  $\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\user shell$ 

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-164e1464-164e1464-164464, \ near \$ 9afe-ea3317b67173}[category]

9afe-ea3317b67173}[name]

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[parentfolder]

Oueries value:

9afe-ea3317b67173}[description]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[relativepath]

Oueries value:

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

Queries value:

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

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e4661-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e461-16e4e46661-16e4e461-16e4e461-16e4e4601-16e4e4661-16e4e461-16e4e461-16e$ 9afe-ea3317b67173}[localizedname] Oueries value:

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

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

 $HKLM \label{lem:hkk} In the latest and the latest$ 9afe-ea3317b67173}[streamresource]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[streamresourcetype]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[localredirectonly]

Queries value:

9afe-ea3317b67173}[roamable]

Oueries value:

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

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1260' \ explorer \ 'folder descriptions' \ 'folder des$ 9afe-ea3317b67173}[stream]

Queries value:

9afe-ea3317b67173}[publishexpandedpath]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[attributes]

Queries value:

9afe-ea3317b67173}[foldertypeid]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ explorer \ 'folder descriptions' \ 'folder desc$ 9afe-ea3317b67173}[initfolderhandler]

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value: 2160590473-689474908-1361669368-1002[profileimagepath]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Queries value:

908e-08a611b84ff6}[category]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-descriptions\} \ for the software \ microsoft \ windows \ for the software \ microsoft \ microso$ 908e-08a611b84ff6}[name]

Queries value:

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

Oueries value:

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

Oueries value:

908e-08a611b84ff6}[relativepath]

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-d14464, and \ baselines \ and \ and \ baselines \ and \ baselines \ and \ baselines \ and \ baselines \ and \ and \ baselines \ and \$ 908e-08a611b84ff6}[localizedname]

Oueries value:

908e-08a611b84ff6}[icon]

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} N $$ \are \microsoft \windows \current version \end{tabular} = \are \cite{local_hammon_ham$ 908e-08a611b84ff6}[security]

908e-08a611b84ff6}[streamresource]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-descriptions'\} \ 'folder \$ 908e-08a611b84ff6}[streamresourcetype]

Queries value:

908e-08a611b84ff6}[localredirectonly]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable] Queries value:

908e-08a611b84ff6}[precreate]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-descriptions\} \ for the software \ microsoft \ windows \ for the software \ microsoft \ microso$ 908e-08a611b84ff6}[stream] Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath] Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes] Oueries value:

 $HKLM \label{lem:hkk} In the latest and the latest$ 908e-08a611b84ff6}[foldertypeid]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `folder descriptions \ `fo$ 908e-08a611b84ff6}[initfolderhandler]

Queries value:

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

folders[cookies]

Oueries value:

a03a-e3ef65729f3d}[category]

Queries value:

a03a-e3ef65729f3d}[name1

a03a-e3ef65729f3d}[parentfolder]

a03a-e3ef65729f3d}[description]

Queries value:

a03a-e3ef65729f3d}[relativepath]

a03a-e3ef65729f3d}[parsingname]

Queries value:

a03a-e3ef65729f3d}[infotip]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}[localizedname]

Oueries value:

a03a-e3ef65729f3d}[icon]

Queries value:

 $HKLM\software\mbox{\sc windows\current} version\explorer\folder descriptions\gamma\folder descriptions\gamma\folder\folder\gamma\folder\folder\gamma\folder\folder\gamma\fol$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \ a03a-e3ef65729f3d \cal{lem:hklmsoftware} \folder \cal{lem:hklmsoftware} \label{lem:hklmsoftware} \ according to \cal{lem:hklmsoftware} \ according \cal{lem:hklms$ 

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{thm:hklm} HKLM\software\mbox{\tt MKLM}\software\mbox{\tt microsoft\windows\currentversion\explorer\folderdescriptions\fold$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \ensurement \ensurements \ensurements \noinder \ensurements \noinder \ensurements \noinder \noin$ 

Oueries value:

Queries value:

 $\label{thm:local-prop} $HKLM \circ ftware \min \circ \current version \explorer \folder descriptions \folder \$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \folder \cal{lem:hklms$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \ensuremath{\tt MK.M} \softw$ 

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]

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

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781 Ea1120a76062\Fralativoaath\

a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-

a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-

a781-5a1130a75963}[infotip]

 $\label{lem:queries} Queries \ value: $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-b784-466-b784-466-b784-466-b784-466-b784-466-b784-466-b784-466-b784-466-b784-466-b784-466-b784-466-b$ 

a781-5a1130a75963}[localizedname]
Oueries value:

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

Queries value:

 $\label{thm:local-bound} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\d9dc8a3b-b784-432e-a781-5a1130a75963\}[security]$ 

Queries value

 $\label{thm:local-prop} HKLM \software \mbox{\current} version \explorer \folder descriptions \folder \descriptions \folder \$ 

Queries value

Queries value.

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

Queries value:

 $\label{thm:local-constraint} HKLM \software \mbox{$d9dc8a3b-b784-432e-a781-5a1130a75963} [local redirectonly]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [roamable]$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\sc} windows \current version \explorer \folder descriptions \folds a 3b-b784-432e-a781-5a1130a75963 \footnote{\sc} [stream]$ 

Queries value:

```
a781-5a1130a75963}[publishexpandedpath]
   Oueries value:
a781-5a1130a75963}[attributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[foldertypeid]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus explorer \setminus \{d9dc8a3b-b784-432e-microsoft \setminus windows \setminus explorer \setminus \{d9dc8a3b-b784-432e-microsoft \setminus explorer \setminus \{d9dc8a4b-b784-432e-microsoft \setminus explorer \setminus \{d9dc8a4b-b784-444b-microsoft \setminus explorer \setminus \{d9dc8a4b-b744b-microsoft \setminus explorer \setminus \{d9dc8a4b-b744b-microsoft \setminus explorer \setminus \{d9dc8a4b-b744b-microsoft \setminus explorer \setminus \{d9dc8a4b-b744b-microsoft 
a781-5a1130a75963}[initfolderhandler]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[history]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\history[cachelimit]
                                                 HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
   Oueries value:
   Oueries value:
                                                 HKLM\software\microsoft\command processor[disableunccheck]
                                                 HKLM\software\microsoft\command processor[enableextensions]
   Oueries value:
   Queries value:
                                                 HKLM\software\microsoft\command processor[delayedexpansion]
   Queries value:
                                                 HKLM\software\microsoft\command processor[defaultcolor]
                                                 HKLM\software\microsoft\command processor[completionchar]
   Queries value:
   Oueries value:
                                                 HKLM\software\microsoft\command processor[pathcompletionchar]
                                                 HKLM\software\microsoft\command processor[autorun]
   Queries value:
   Queries value:
                                                 HKCU\software\microsoft\command processor[disableunccheck]
                                                 HKCU\software\microsoft\command processor[enableextensions]
   Queries value:
   Queries value:
                                                 HKCU\software\microsoft\command processor[delayedexpansion]
   Queries value:
                                                 HKCU\software\microsoft\command processor[defaultcolor]
   Queries value:
                                                 HKCU\software\microsoft\command processor[completionchar]
   Oueries value:
                                                 HKCU\software\microsoft\command processor[pathcompletionchar]
    Oueries value:
                                                 HKCU\software\microsoft\command processor[autorun]
    Queries value:
                                                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
    Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [default level]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[saferflags]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\srp\gp[rulecount]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
   Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [log filename]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                                                 \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt defined} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mb
   Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
   Oueries 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]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                                 \label{thm:linear} \mbox{HKCU\software\mbox{$\stackrel{\cdot}{m}$icrosoft\windows\currentversion\internet}} \\
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                                 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries 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]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
   Queries value:
                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
   Queries value:
                                                 \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
   Queries value:
                                                 \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
   Queries value:
                                                 \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
   Queries value:
                                                 \label{local-condition} \mbox{HKCU\software\policies\mbox{$\mbox{microsoft\windows\currentversion\internet}$} \label{local-condition}
settings[enableautoproxyresultcache]
   Queries value:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
```

```
settings[displayscriptdownloadfailureui]
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[mbcsservername]
  Queries value:
                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
  Queries value:
                                       \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[utf8servernameres]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Oueries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketsendbufferlength]
  Oueries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[keepalivetimeout]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxhttpredirects]
                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[maxconnectionsperserver]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsperserver]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[maxconnectionsper1_0server]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[maxconnectionsperproxy]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                                       \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} internet \end{tabular}
  Queries value:
settings[connectretries]
                                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
  Queries value:
settings[sendtimeout]
                                       \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} internet \end{tabular}
  Queries value:
settings[sendtimeout]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[disablentlmpreauth]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certcachenovalidate]
  Oueries 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]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[httpdefaultexpirytimesecs]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[ftpdefaultexpirytimesecs]
                                       HKLM\software\microsoft\internet
  Queries value:
explorer \\ \verb|main| feature control| feature_disable_unicode_handle_closing_callback [81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe] \\ explorer \\ explorer
                                       HKLM\software\microsoft\internet
  Queries value:
explorer \verb|\main| feature_disable_unicode_handle_closing_callback[*]|
  Queries value:
                                       \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[disablecachingofsslpages]
  Oueries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
  Queries value:
settings[dialupuselansettings]
  Queries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendextracrlf]
  Queries value:
                                       \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \colongraph internet
settings[wpadsearchalldomains]
  Queries value:
                                       \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[bypasshttpnocachecheck]
  Queries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Oueries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:
                                       HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
```

HKLM\software\microsoft\windows\currentversion\internet

Queries value:

```
settings[enablehttptrace]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                           \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
 Queries value:
settings[headerexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheenabled]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonzonecrossing]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost
                     redirect]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM \verb|\system| current control \verb|\space| control \verb|\space| lsa \verb|\accessproviders| [marta extension]|
 Queries value:
                           HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
                           HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Queries value:
 Queries value:
                           HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
                           \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
 Queries value:
settings\wpad[wpadoverride]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[enableautodial]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[globaluseroffline]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
 Oueries value:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\cache[persistent]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\cache[persistent]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\cache[persistent]
 Oueries value:
                           HKLM\software\microsoft\windows\html help[.hlp]
                           HKCU\software\microsoft\windows\currentversion\run[wincl]
 Sets/Creates value:
```

HKCU\software\vb and vba program settings\clock\sdata[s]

Sets/Creates value: