# Malware Analysis Appliance by Blue Coat Systems, Inc.

Host: mag2, Sample ID: 11, Task ID: 44

Task Details

Task ID: 44 Risk Level:

Date Processed: 2016-04-28 12:47:01 (UTC)

Processing Time: 62.37 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe"

Sample ID: Type: basic Owner: admin

83497c45d30bcb551f5f55f3f63b6fa1 Label: 2016-04-28 12:44:50 (UTC) Date Added:

PE32:win32:gui File Type:

File Size: 892928 bytes

83497c45d30bcb551f5f55f3f63b6fa1 MD5:

SHA256: 40932ac88b750f1f3077f2e50d9184de1c3b4914e92ceb64cfc4638c3d91ee14

Description: None

### Pattern Matching Results

3 Long sleep detected

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

3 Connects to local host

4 Checks whether debugger is present

#### Process/Thread Events

C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe Creates process:

["C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe"]

### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex

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

Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex

\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: Creates mutex:  $\verb|\Sessions|1| BaseNamedObjects| ZonesLockedCacheCounterMutex|$ 

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

Creates mutex:

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

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:  $\verb|\Sessions|1| BaseNamedObjects| WininetStartupMutex|$ Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex Creates mutex: Creates mutex:  $\verb|\Sessions|1\BaseNamedObjects| CicLoadWinStaWinStaO|$ 

\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

\Sessions\1\BaseNamedObjects\!IETld!Mutex Creates mutex:  $\verb|\Sessions|1\BaseNamedObjects| RasPbFile| \\$ Creates mutex:

Creates mutex:  $\verb|\Sessions|1| BaseNamedObjects| MSIMGSIZEC acheMutex|$ 

Creates mutex:

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

Creates event: \KernelObiects\MaximumCommitCondition \Security\LSA AUTHENTICATION INITIALIZED Creates event:

Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX

\BaseNamedObjects\BFE\_Notify\_Event\_{7fd7dd57-48d8-4cba-b3f7-Creates event:

ee4709cc60f9}

## File System Events

Creates: C:\Users\Admin

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

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

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

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

Files\Content.IE5\TZILKL9J\104[1]

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

Files\Content.IE5\266VNL5S\property\_front[1].aspx

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

Files\Content.IE5\266VNL5S\JMX.Frame.Common[1].js

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

Files\Content.IE5\VB8EH8F1\jquery-1.4.2.min[1].js

```
C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates
Files\Content.IE5\VB8EH8F1\JMX_FormValidator[1].js
 Creates:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\JMX_AjaxControl[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\266VNL5S\client_ending[1].htm
 Creates
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\SRO-ending[1].jpg
 Creates
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\btn_facebook[1].jpg
 Opens:
                         C:\Windows\Prefetch\83497C45D30BCB551F5F55F3F63B6-CCFC2B0F.pf
 Opens:
                         C:\Windows
 Opens:
                         C:\Windows\System32\wow64.dll
                         C:\Windows\System32\wow64win.dll
 Opens:
 Opens:
                         C:\Windows\System32\wow64cpu.dll
 Opens:
                         C:\Windows\system32\wow64log.dll
 Opens:
                         C:\Windows\SysWOW64
 Opens:
                         C:\Windows\SysWOW64\sechost.dll
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Local\
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
 Opens:
                         C:\windows\temp\WINSPOOL.DRV
 Opens:
                         C:\Windows\SysWOW64\winspool.drv
 Opens:
                         C:\windows\temp\oledlg.dll
 Opens:
                         C:\Windows\SysWOW64\oledlg.dll
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C: \verb|\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.2.Manifest|
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.3.Manifest
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Config
 Opens:
                         C:\Windows\Temp\83497c45d30bcb551f5f55f3f63b6fa1.exe
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.1000.Manifest
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1ENU.dll
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1LOC.dll
 Opens:
                         C:\Windows\Fonts\tahoma.ttf
 Opens:
                         C:\windows\temp\dwmapi.dll
 Opens:
                         C:\Windows\SysWOW64\dwmapi.dll
 Opens:
                         C:\Windows\winhlp32.exe
 Opens:
                         C:\Windows\SysWOW64\rpcss.dll
 Opens:
                         C:\Windows\SysWOW64\ieframe.dll
                         C:\Windows\SysWOW64\oleacc.dll
 Opens:
 Opens:
                         C:\windows\temp\OLEACCRC.DLL
 Opens:
                         C:\Windows\SysWOW64\oleaccrc.dll
 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
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
                         C:\windows\temp\apphelp.dll
 Opens:
                         C:\Windows\SysWOW64\apphelp.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\ieframe.dll.mui
 Opens:
                         C:\Windows\SysWOW64\mshtml.dll
 Opens:
                         C:\Windows\SysWOW64\msls31.dll
                         C:\Windows\SysWOW64\version.dll
 Opens:
 Opens:
                         C:\windows\temp\ntmarta.dll
 Opens:
                         C:\Windows\SysWOW64\ntmarta.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe:Zone.Identifier
 Opens:
                         C:\windows\temp\profapi.dll
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Roaming
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
```

```
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\windows\temp\dnsapi.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\windows\temp\iphlpapi.DLL
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
 Opens:
                         C:\windows\temp\WINNSI.DLL
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\TZILKL9J\104[1]
                         C:\Windows\SysWOW64\en-US\urlmon.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
                         C:\windows\temp\RASAPI32.dll
 Opens:
                         C:\Windows\SysWOW64\rasapi32.dll
 Opens:
 Opens:
                         C:\windows\temp\rasman.dll
                         C:\Windows\SysWOW64\rasman.dll
 Opens:
 Opens:
                         C:\windows\temp\rtutils.dll
 Opens:
                         C:\Windows\SysWOW64\rtutils.dll
 Opens:
                         C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\Windows\SysWOW64\ras
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\windows\temp\sensapi.dll
 Opens:
                         C:\Windows\SysWOW64\SensApi.dll
 Opens:
                         C:\Windows\SysWOW64\nlaapi.dll
 Opens:
                         C:\windows\temp\rasadhlp.dll
 Opens:
                         C:\Windows\SysWOW64\rasadhlp.dll
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wship6.dll
 Opens:
                         C:\Windows\SysWOW64\msimtf.dll
 Opens:
                         C:\windows\temp\MLANG.dll
 Opens:
                         C:\Windows\SysWOW64\mlang.dll
 Opens:
                         C:\Windows\Fonts\times.ttf
 Opens:
                         C:\windows\temp\dhcpcsvc6.DLL
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
                         C:\windows\temp\dhcpcsvc.DLL
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
                         C:\Windows\System32\drivers\etc\hosts
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.DLL
                         C:\Windows\System32\C_20127.NLS
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\property_front[1].aspx
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\266VNL5S\JMX.Frame.Common[1].js
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\JMX_FormValidator[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.4.2.min[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\TZILKL9J\JMX_AjaxControl[1].js
                         C:\Windows\SysWOW64\jscript.dll
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\windows\temp\RpcRtRemote.dll
 Opens:
                         C:\Windows\SysWOW64\RpcRtRemote.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\jscript.dll.mui
                         C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\266VNL5S\client_ending[1].htm
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\Windows\SysWOW64\en-US\mshtml.dll.mui
 Opens:
 Opens:
                         C:\Windows\Fonts\StaticCache.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
                         \verb|C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat|\\
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\104[1]
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\266VNL5S\property_front[1].aspx
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\JMX.Frame.Common[1].js
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\JMX_FormValidator[1].js
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\jquery-1.4.2.min[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\TZILKL9J\JMX_AjaxControl[1].js
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\client_ending[1].htm
 Writes to:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

Files\Content.IE5\266VNL5S\SRO-ending[1].jpg

Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\WM60WM90\btn\_facebook[1].jpg

C:\Windows\System32\drivers\etc\hosts Reads from:

Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\VB8EH8F1\jquery-1.4.2.min[1].js

Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\VB8EH8F1\JMX\_FormValidator[1].js

Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\TZILKL9J\JMX\_AjaxControl[1].js

 $\hbox{\tt C:\backslash Users\backslash Admin\backslash AppData\backslash Local\backslash Microsoft\backslash Windows\backslash Temporary\ Internet}$ Reads from:

Files\Content.IE5\266VNL5S\JMX.Frame.Common[1].js

Reads from: C:\Windows\Fonts\StaticCache.dat

#### Network Events

DNS query: www.joymax.com DNS query: file.joymax.com DNS query: silkroadcp.joymax.com

DNS query: img.joymax.com

DNS response: www.joymax.com ⇒ 222.111.176.232 DNS response: file.joymax.com  $\Rightarrow$  222.111.176.232 DNS response: silkroadcp.joymax.com ⇒ 121.128.133.11 DNS response: silkroadcp.joymax.com ⇒ 121.128.133.12 DNS response:  $img.joymax.com.gccdn.net \Rightarrow 119.31.253.194$ DNS response: img.joymax.com.gccdn.net ⇒ 14.0.55.11

Connects to: 127.0.0.1:54605 Connects to: 222.111.176.232:80 Connects to: 121.128.133.11:80 Connects to: 119.31.253.194:80 Sends data to: 8.8.8.8:53 Sends data to: 127.0.0.1:54605

file.joymax.com:80 (222.111.176.232) Sends data to: Sends data to: silkroadcp.joymax.com:80 (121.128.133.11) Sends data to: img.joymax.com.gccdn.net:80 (119.31.253.194)

Receives data from: 8.8.8.8:53 Receives data from: 127.0.0.1:54605

Receives data from: file.joymax.com:80 (222.111.176.232) silkroadcp.joymax.com:80 (121.128.133.11) Receives data from: Receives data from: img.joymax.com.gccdn.net:80 (119.31.253.194)

#### Windows Registry Events

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

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

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32 Creates kev:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus tracing \setminus 83497 \\ c45d30bcb \\ 551f5f55f3f63b6fa1\_rasmancs$ Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\connections

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

awareness

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters HKCU\software\microsoft\windows\currentversion\internet Creates key:

settings\p3p\history

Creates key: HKCU\software\microsoft\windows script\settings

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

settings\zonemap[proxybypass]

Deletes value:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ 

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

HKI M\software\wow6432node\microsoft\windows\currentversion\internet Deletes value:

settings\zonemap[intranetname]

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

settings[proxyserver]

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

settings[proxyoverride] Deletes value:

HKCU\software\microsoft\windows\currentversion\internet

settings[autoconfigurl]

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

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

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

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens kev: HKLM\system\currentcontrolset\control\mui\uilanguages HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings HKLM\software\policies\microsoft\mui\settings Opens key: Opens key: HKCU\ Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key:

HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

HKCU\control panel\desktop\muicached Opens key:

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

Opens key:

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

Opens key:

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

nt\currentversion\diagnostics

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

nt\currentversion\gre\_initialize

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

nt\currentversion\compatibility32

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

compatibility

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

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

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

HKCU\software\classes\ Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid

Opens key: HKCR\wow6432node\clsid

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

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\network Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKLM\system\currentcontrolset\control\nls\locale  $HKLM \ system \ current controls et \ control \ nls \ locale \ alternate \ sorts$ Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: Opens key: HKLM\software\microsoft\com3

HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\treatas

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-11d0-a96b-1440a-144$ Opens key:

00c04fd705a2}\inprochandler32

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}\inprochandler

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

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

Opens key: HKLM\system\setup

 $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows | nt\\| rpc$ 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: HKLM\system\currentcontrolset\services\crypt32

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

settings Opens key:

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

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

settings

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

settings

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_http\_username\_password\_disable

HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_http\_username\_password\_disable

HKLM\software\wow6432node\policies\microsoft\internet Opens kev:

explorer\main\featurecontrol

Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key:  $\label{lem:hkcu} \verb+KKCU\software\policies\microsoft\internet\ explorer\main\feature control$ 

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

explorer\main\featurecontrol

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

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562

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

explorer\main\featurecontrol\feature\_allow\_reverse\_solidus\_in\_userinfo\_kb932562

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

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

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

Opens key:

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

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 83497c45d30bcb551f5f55f3f63b6fa1. execution \ shell \ compatibility \ applications \ applications \ shell \ compatibility \ applications \ app$ 

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\shellfolder

HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-Opens key:

08002b30309d}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-

42a0-1069-a2ea-08002b30309d}\shellfolder

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

Opens key:

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

Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32

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

extensions\blocked

Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked  ${\tt HKLM \ } system \verb|\ current control \ } session \ manager \verb|\ app compatibility|$ Opens key:

Opens key:  $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| appcompat$ 

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

HKCU\software\microsoft\windows\currentversion\shell extensions\cached Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d} Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\treatas

HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\progid

HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid Opens key: Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d} Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\progid

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-Opens key:

08002b30309d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-Opens key:

08002b30309d}\inprochandler

HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-Opens key:

08002b30309d}\inprochandler

Opens key:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{le$ 

42a0-1069-a2ea-08002b30309d}

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_iedde\_register\_protocol

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

explorer\main\featurecontrol\feature iedde register protocol

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

explorer\browseremulation

HKLM\software\policies\microsoft\internet explorer\browseremulation Opens kev:  $\label{lem:hkcu} \mbox{HKCU\software\policies\mbox{$\mbox{microsoft\internet}$ explorer\browseremulation}} \label{lem:hkcu}$ Opens key:

Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKCU\software\classes\protocols\name-space handler\

Opens key: HKCR\protocols\name-space handler

Opens key: HKCU\software\classes\protocols\name-space handler\res\

HKCR\protocols\name-space handler\res Opens kev:

Opens key: HKCU\software\classes\protocols\name-space handler\\*\

HKCR\protocols\name-space handler\\* Opens key: HKCU\software\classes\protocols\handler\res Opens key: Opens kev: HKCR\protocols\handler\res Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\treatas HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\progid  $HKCR \setminus wow6432 node \\ clsid \\ \{3050f3bc-98b5-11cf-bb82-00aa00bdce0b\} \\ \setminus progid$ Opens key: Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f3bc-98b5-11cf-bb82-11c$ Opens key: 00aa00bdce0b}\progid Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandler Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_aria\_support HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_aria\_support Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_legacy\_dispparams HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_legacy\_dispparams HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_private\_font\_setting HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_private\_font\_setting Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_css\_show\_hide\_events Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_css\_show\_hide\_events HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_display\_node\_advise\_kb833311 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_display\_node\_advise\_kb833311 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_allow\_expanduri\_bypass Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_allow\_expanduri\_bypass Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_body\_size\_in\_editable\_iframe\_kb943245 HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_body\_size\_in\_editable\_iframe\_kb943245 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_databinding\_support Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_databinding\_support Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_enforce\_bstr HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature enforce bstr Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_enable\_dynamic\_object\_caching Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_enable\_dynamic\_object\_caching

explorer\main\featurecontrol\feature\_object\_caching Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_object\_caching

Opens kev:

HKCU\software\microsoft\internet

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_legacy\_tostring\_in\_compatview

```
HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens kev:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens kev:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
  Opens key:
                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
  Opens kev:
                                     HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
                                      HKLM\software\wow6432node\microsoft\windows\currentversion\app
  Opens key:
paths\outlook.exe
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens key:
                                      HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility
  Opens key:
                                      HKLM\software\wow6432node\policies\microsoft\internet
explorer\domstorage
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                      HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                      HKCU\software\microsoft\internet explorer\domstorage
                                      HKLM\software\wow6432node\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                      HKLM\software\wow6432node\policies\microsoft\internet
explorer\safety\privacie
                                     HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens kev:
  Opens key:
                                      HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                      HKCU\software\microsoft\internet explorer\safety\privacie
                                      HKLM\software\wow6432node\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                      Opens key:
                                      HKLM\system\currentcontrolset\services\ldap
                                      \label{local-observation} \mbox{HKLM} \\ \mbox{$\stackrel{\circ}{\mbox{software}}$ \ensuremath{\mbox{wow}6432}$ node\\ \mbox{$\stackrel{\circ}{\mbox{microsoft}}$ internet explorer\\ \mbox{$\stackrel{\circ}{\mbox{mediatypeclass}}$ }
  Opens key:
  Opens key:
                                      settings\accepted documents
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\policies\ratings
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:
                                     HKLM\software\wow6432node\policies
  Opens key:
                                      HKCU\software\policies
                                     HKCU\software
  Opens key:
  Opens key:
                                      HKLM\software\wow6432node
  Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
                                      HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature ignore policies zonemap if esc enabled kb918915
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens kev:
HKLM \verb|\software| wow 6432 node \verb|\policies| microsoft| windows \verb|\currentversion| internet| and the software \verb|\currentversion| internet and the software and the software \verb|\currentversion| internet and the software and the s
settings\zonemap\domains\
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\ranges
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
```

Opens key:

settings\zonemap

 $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt hicrosoft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\current\windows\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\wi$ 

```
settings\zonemap
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\ranges\
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
  Opens key:
                                     \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\zonemap\domains\
  Opens key:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                     HKLM\software\wow6432node\policies\microsoft\internet explorer
                                     HKLM\software\policies\microsoft\internet explorer
  Opens key:
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer\security
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\
                                     \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl} zones \end{\tt 0}
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens kev:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ zones \ \ windows \ construction \ the settings \ before \ the settings \ t
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones\
  Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ vones \ \ 0
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\0
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\0
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\1
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\1
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens kev:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens kev:
Opens key:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\3
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones\3
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\4
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown
                                     HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:
HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\
  Opens kev:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\0
  Opens kev:
settings\lockdown_zones\0
  Opens key:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\0
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\1
  Opens key:
settings\lockdown_zones\1
```

```
Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown zones\3
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\4
 Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\4
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                        HKCU\software\classes\protocols\name-space handler\c\
 Opens key:
 Opens key:
                        HKCR\protocols\name-space handler\c
 Opens key:
                        HKCU\software\classes\protocols\handler\c
 Opens key:
                        HKCR\protocols\handler\c
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
HKLM \verb|\software\\| \verb|\windows\\| current version\\| explorer\\| folder descriptions
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
 Opens kev:
33be-4251-ba85-6007caedcf9d}\propertybag
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\explorer
                        HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
 Opens kev:
 Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follown folders
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
 Opens key:
c0e9-4171-908e-08a611b84ff6}
 Opens key:
c0e9-4171-908e-08a611b84ff6}\propertybag
 Opens key:
                        HKCU\software\microsoft\internet explorer
                        HKLM\software\wow6432node\microsoft\internet explorer
 Opens key:
                        HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_mime_handling
                        HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature mime handling
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
 Opens kev:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature load shdoclc resources
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                        HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
 Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
```

HKLM\software\wow6432node\microsoft\internet

Opens key:

explorer\main\featurecontrol\feature\_feeds

Opens key: HKCU\software\classes\protocols\filter\text/html

Opens key: HKCR\protocols\filter\text/html

Opens key: 

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

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

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

Opens key:

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

Opens key:

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

Opens key:

0e22-4760-9afe-ea3317b67173}

Opens key:

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

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

nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

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

980053277-1733835069-2361817685-1001

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (3eb685db-10eb) \ description \ (3eb685db-10eb) \$ 65f9-4cf6-a03a-e3ef65729f3d}

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}\propertybag

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

settings\5.0\cache\history

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

settings\5.0\cache\history

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d12b, d12b, d24b, d$ b784-432e-a781-5a1130a75963}

Opens key:

b784-432e-a781-5a1130a75963}\propertybag

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\extensible cache\feedplat

Opens key:

HKCU\software\microsoft\windows\currentversion\internet 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 kev: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset

HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_bufferbreaking\_818408

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

explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache

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

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\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                       HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                       HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                       HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                       HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                       HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                       HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens kev:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                       HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature release keys on unload kb975619
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens kev:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens kev:
                       HKLM\system\currentcontrolset\services\winsock2\parameters
                       HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ appid\_catalog
 Opens key:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\14993e33
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000010

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

Opens kev:

Opens key:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
    Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 00000000000001) \ (catalog\_entries \ name space\_catalog 5) \ (catalog\_entries 
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
    Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\internet settings\wpad
                                                           HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
    Opens key:
                                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
    Opens key:
                                                           HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
    Opens key:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
    Opens key:
                                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
                                                          HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Opens key:
00aa00686f13}
    Opens key:
                                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
    Opens kev:
                                                           HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
    Opens key:
                                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
    Opens key:
                                                           HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
    Opens key:
                                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
                                                           HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
    Opens key:
00aa00686f13}\inprocserver32
   Opens key:
                                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
                                                           HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 11cf
    Opens key:
00aa00686f13}\inprochandler32
                                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
    Opens key:
00aa00686f13}\inprochandler32
                                                           HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Opens kev:
00aa00686f13}\inprochandler
                                                           HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
    Opens key:
00aa00686f13}\inprochandler
                                                           HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_manage_script_circular_refs
   Opens kev:
                                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
                                                           HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature restrict filedownload
    Opens key:
                                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
   Opens key:
                                                           HKLM\software\wow6432node\microsoft\internet explorer\security\floppy
access
    Opens key:
                                                           HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
                                                           HKLM\software\wow6432node\microsoft\internet explorer\security\adv
    Opens key:
addrbar spoof detection
    Opens key:
                                                           HKCU\software\classes\protocols\name-space handler\about\
    Opens key:
                                                           HKCR\protocols\name-space handler\about
    Opens key:
                                                           HKCU\software\classes\protocols\handler\about
    Opens key:
                                                           HKCR\protocols\handler\about
                                                           HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
    Opens key:
00aa00bdce0b}
    Opens key:
                                                           HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
                                                           HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{3050f406 - 98b5 - 11cf - bb82 - bb82
    Opens key:
00aa00bdce0b}\treatas
    Opens key:
                                                           HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
    Opens key:
                                                           HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
    Opens key:
                                                           HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
                                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f406-98b5-11cf-bb82-00aa00bdce0b\}
    Opens key:
    Opens key:
                                                           HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
    Opens key:
                                                           HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\progid
                                                           HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid
    Opens kev:
    Opens key:
                                                           HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
    Opens key:
                                                           HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
```

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{3050f406 - 98b5 - 11cf - bb82 - bb82 - 11cf - bb82 - bb82$ 

Opens key:

00aa00bdce0b}\inprochandler32 HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandler Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_document\_compatible\_mode HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_document\_compatible\_mode Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_protocol\_lockdown Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\zoom Opens key: HKLM\software\policies\microsoft\internet explorer\zoom Opens key: HKCU\software\policies\microsoft\internet explorer\zoom Opens key: HKCU\software\microsoft\internet explorer\zoom HKLM\software\wow6432node\microsoft\internet explorer\zoom Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_weboc\_document\_zoom Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_ipersistmoniker\_load\_redirected\_url\_kb976425 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_ipersistmoniker\_load\_redirected\_url\_kb976425 Opens kev: HKCU\software\policies\microsoft\internet explorer Opens key: HKCU\software\microsoft\internet explorer\international Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts Opens key: HKCU\software\microsoft\internet explorer\international\scripts Opens key: HKLM\software\wow6432node\microsoft\internet explorer\international\scripts Opens key: HKLM\software\policies\microsoft\internet explorer\settings Opens key: HKCU\software\microsoft\internet explorer\settings Opens key: HKLM\software\wow6432node\microsoft\internet explorer\settings Opens key: HKCU\software\microsoft\internet explorer\styles Opens key: HKCU\software\microsoft\windows\currentversion\policies\activedesktop Opens key: HKCU\software\microsoft\windows\currentversion\policies HKCU\software\microsoft\internet explorer\pagesetup Opens key: Opens key:  $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc menuext}} \\$ Opens key: HKCU\software\microsoft\internet explorer\menuext\%s HKLM\system\currentcontrolset\control\nls\codepage Opens key: Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog HKLM\software\wow6432node\microsoft\internet explorer\version vector Opens kev: HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_zone\_elevation Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_sslux HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_sslux Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\zones\0 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_xssfilter Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_xssfilter HKCU\software\microsoft\windows\currentversion\internet settings\zones Opens key: Opens key: HKLM\software\policies\microsoft\internet explorer\low rights Opens key: HKCU\software\microsoft\internet explorer\low rights  $\label{lem:hklm} \mbox{HKLM\software\wow6432} node\mbox{\sweether} icrosoft\space{-0.05\lineskip} internet explorer\space{-0.05\lineskip} lower\space{-0.05\lineskip} internet explorer\space{-0.05\lineskip} lower\space{-0.05\lineskip} lower\space{-0.05\$ Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_read\_zone\_strings\_from\_registry Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_read\_zone\_strings\_from\_registry Opens kev: settings\zones\1 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\2

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

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

Opens key: settings\zones\3 Opens key:

settings\zones\4

```
Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus compatibility \setminus 83497 \\ c45d30bcb551f5f55f3f63b6fa1.exe
                                                              HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07
    Opens kev:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
    Opens kev:
                                                              HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                              HKLM\software\wow6432node\microsoft\ctf\
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\ctf\knownclasses
    Opens key:
    Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
    Opens kev:
                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe
    Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
                                                              HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| internet
    Opens key:
explorer\main\featurecontrol\feature_enable_compat_logging
                                                              HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
    Opens key:
                                                             HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
    Opens key:
                                                              HKCU\software\microsoft\internet explorer\ietld
    Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
    Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus tracing \setminus 83497 \\ c45d30bcb551f5f55f3f63b6fa1\_rasapi32
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
    Opens key:
                                                              HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
    Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ 163b6fa1\_rasmancs $$ 163b6fa1\_rasmancs
    Opens key:
                                                              HKLM\software\microsoft\sqmclient\windows\disabledsessions\
    Opens key:
                                                              HKLM\system\currentcontrolset\control\sqmservicelist
    Opens key:
    Opens key:
                                                              {\tt HKLM \ } system \verb| current control set \verb| services \verb| dns cache \verb| parameters | \\
    Opens key:
                                                              HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
    Opens key:
                                                              HKLM\software\policies\microsoft\windows nt\dnsclient
    Opens key:
                                                              HKLM\system\currentcontrolset\services\dns
    Opens key:
                                                              HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
    Opens key:
                                                              HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
    Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
    Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_isolate_named_windows
                                                              HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_isolate_named_windows
                                                              HKCU\software\microsoft\internet
    Opens kev:
explorer\main\featurecontrol\feature_binary_caller_service_provider
                                                              HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature binary caller service provider
    Opens key:
                                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\url history
    Opens kev:
                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\url history
                                                              HKCU\software\microsoft\windows\currentversion\internet settings\url
    Opens key:
history
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history
    Opens key:
                                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_codepage_inherit
                                                              HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_codepage_inherit
    Opens key:
                                                              HKCU\software\classes\protocols\name-space handler\http\
    Opens key:
                                                              HKCR\protocols\name-space handler\http
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\user agent
    Opens key:
                                                              \label{lem:hklmsoftware policies microsoft windows \current version \cite{thmsoftware} in the lemma of the 
settings\user agent
    Opens key:
                                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user agent
    Opens key:
                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\ua tokens
```

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

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

Opens key:

settings\user agent\pre platform

```
settings\5.0\user agent\pre platform
```

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

settings\5.0\user agent\pre platform

Opens key:

settings\user agent\post platform

Opens key: 

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

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

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

explorer\main\featurecontrol\feature\_maxconnectionsperserver HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_maxconnectionsper1\_0server HKLM\software\wow6432node\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_maxconnectionsper1\_0server Opens key: HKLM\system\currentcontrolset\services\winsock\parameters

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

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

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

migration\providers\tcpip

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209 HKCU\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature\_disable\_legacy\_compression Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_disable\_legacy\_compression

Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - a8dc - 47f3 - 800f - 800f$ 

fd2b31b3eefd}

Opens key: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd} Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\treatas

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\progid

Opens key:  $HKCR\wow6432 node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\\progid$ Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}

Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd} HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-Opens key:

fd2b31b3eefd}\progid

Opens key:  $HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid$ 

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - a8dc - 47f3 - 800f - 800f$ Opens key:

fd2b31b3eefd}\inprocserver32

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-Opens kev:

fd2b31b3eefd}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-Opens key:

fd2b31b3eefd}\inprochandler32

Opens key:

fd2b31b3eefd}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandler

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-Opens key:

fd2b31b3eefd}\inprochandler

HKCU\software\classes\protocols\name-space handler Opens key:

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

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

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

migration\providers\tcpip6

Opens key:

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

settings\zonemap\

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

explorer\restrictions

HKLM\software\policies\microsoft\internet explorer\restrictions Opens key: Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-Opens kev:

f4ceaaf59cfc}\treatas

Opens key:  $HKCR\wow6432 node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treat as$ Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\progid

Opens key:  $HKCR \setminus wow6432 node \\ clsid \\ \{50d5107a-d278-4871-8989-f4ceaaf59cfc\} \\ \setminus progid$ HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens kev:

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}

Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\progid HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-Opens key: f4ceaaf59cfc}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprochandler32 Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient HKLM\software\policies\microsoft\system\dnsclient Opens key: Opens key: Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprochandler32 Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d278$ f4ceaaf59cfc}\inprochandler Opens kev: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989f4ceaaf59cfc}\inprochandler Opens key: HKCU\software\policies\microsoft\internet explorer\control panel HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_iedde\_register\_urlecho Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_iedde\_register\_urlecho HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5} Opens key: HKLM\software\policies\microsoft\internet explorer\recovery Opens key: HKCU\software\microsoft\internet explorer\recovery Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5} Opens key: HKCU\software\microsoft\internet explorer\feed discovery Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ internet\ explorer \ feed\ discovery$ Opens key: HKCU\software\microsoft\ftp Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963} Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963} HKLM\svstem\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-127795cce47a} 65fee5bae0b1}  ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ linkage \\$ Opens key: HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\p3p\history\joymax.com HKCU\software\classes\mime\database\content type\text/html; charset=utf-Opens key: 8 HKCR\mime\database\content type\text/html; charset=utf-8 Opens key: HKCU\software\classes\mime\database\content type\text/html Opens key: HKCR\mime\database\content type\text/html Opens kev: Opens key: HKCU\software\classes\protocols\filter\text/html; charset=utf-8 HKCR\protocols\filter\text/html; charset=utf-8 Opens kev: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown Opens key: HKCU\software\classes\mime\database\content type\application/xjavascript Opens kev: HKCR\mime\database\content type\application/x-javascript HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_custom\_image\_mime\_types\_kb910561

explorer\main\featurecontrol\feature\_custom\_image\_mime\_types\_kb910561

Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature\_custom\_image\_mime\_types\_kb910561

Opens key: HKCU\software\microsoft\internet

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_block\_lmz\_script

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

 $\verb|explorer\main\featurecontrol\feature_block_lmz_script| \\$ 

Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}

00aa00bbbb58}\treatas

00aa00bbbb58}\progid

Opens key:  $\begin{tabular}{ll} HKCR \begin{tabular}{ll} HKCR \begin{tabular}{ll} HKCR \begin{tabular}{ll} HKCU \software \classes \software \classes \begin{tabular}{ll} HKCU \software \classes \software \software \classes \software \softwar$ 

00aa00bbbb58}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprochandler

Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprochandler

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

Opens key: HKCU\software\microsoft\internet

Opens key: HKLM\software\wow6432node\microsoft\com3

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

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

Opens key: HKCU\software\classes\appid\83497c45d30bcb551f5f55f3f63b6fa1.exe

Opens key: HKCR\appid\83497c45d30bcb551f5f55f3f63b6fa1.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat

Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrol\set\control\lsa

Opens key:

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic

provider

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

Opens key:

 $\label{lem:hklmsystem} HKLM \space{$\operatorname{Microsoft\cryptography\configuration}$} Opens \ key: \\ HKLM \space{$\operatorname{Microsoft\cryptography}$}$ 

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload

00000000046}

 $000000000046 \} \verb|\proxystubclsid32|$ 

Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-

00000000046}\proxystubclsid32

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_use\_windowedselectcontrol
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature\_use\_windowedselectcontrol

Opens key: HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}

 $\label{lem:openskey: HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b\}} \\ \mbox{Opens key:} HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b\}} \\ \mbox{Opens key:} \mbox{HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b\}}} \\ \mbox{Opens key:} \mbox{Openskey:} \mbox{HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b\}}} \\ \mbox{Openskey:} \mbox{Opensk$ 

00aa00bdce0b}\treatas

00aa00bdce0b}\progid

 $\label{lem:opensky: hkcrwow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\progid Opensky: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}$ 

Opens key: HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\progid

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCR} \\ \mathsf{Clsid} \\ \{3050f391-98b5-11cf-bb82-00aa00bdce0b\} \\ \mathsf{progid} \\$ 

Opens key: HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler

Opens key: HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_xmlhttp

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

explorer\main\featurecontrol\feature\_xmlhttp

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_restrict\_about\_protocol\_ie7

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

explorer\main\featurecontrol\feature\_restrict\_about\_protocol\_ie7

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

Opens key: HKCU\software\microsoft\internet explorer\dxtrans

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_scripturl\_mitigation

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

explorer\main\featurecontrol\feature\_scripturl\_mitigation
 Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature\_block\_lmz\_img

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

explorer\main\featurecontrol\feature\_block\_lmz\_img

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore\_v1.0

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms shell dlg

Opens key: HKCU\software\classes\mime\database\content type\image/jpeg

Opens key: HKCR\mime\database\content type\image/jpeg

Opens key:  ${\tt HKLM\backslash software\backslash policies\backslash microsoft\backslash internet\ explorer\backslash services}$ 

Opens key: HKCU\software\microsoft\internet explorer\services

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

Opens key: HKCU\software\microsoft\internet explorer\activities

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

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

Opens key: HKCU\software\microsoft\internet explorer\suggested sites

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Queries value:

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

Queries value:

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

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

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

us[alternatecodepage]

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

 $\label{thm:linear} Queries\ value: \\ HKCU \ control\ panel \ desktop \ muicached \ [machine preferred uil anguages]$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

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

Queries value: HKLM\system\currentcontrol\setsion manager[safedllsearchmode]

 $\label{lem:prop:continuous} Queries \ value: \ HKLM\software\mbox{\sc microsoft\sc windows} \\ nt\c current version\sc gre_initialize\sc [disablemetafiles]$ 

 $Queries\ value: \ HKLM\ software\ wow 6432 node\ microsoft\ windows \\ nt\ current version\ compatibility 32 [83497c45d30bcb551f5f55f3f63b6fa1]$ 

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit\_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]

Queries value: HKLM\system\currentcontrol\set\control\nls\language groups[1]

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

Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]

Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]

Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxxxshashcount]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Oueries value:

```
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                                HKLM\svstem\setup[oobeinprogress]
   Oueries value:
   Oueries value:
                                                HKLM\system\setup[systemsetupinprogress]
   Queries value:
                                                HKLM\software\microsoft\sqmclient\windows[ceipenable]
                                                HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Oueries value:
   Queries value:
                                                HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[disableimprovedzonecheck]
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[security_hklm_only]
   Queries value:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value:
                                                \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt hicrosoft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\wi
settings[createuricachesize]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Queries value:
settings[createuricachesize]
   Queries value:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                                \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt hicrosoft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt lem:hkcu\soft\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\current\windows\current\windows\current\windows\current\windows\current\windows\current\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\windows\wi
   Queries value:
settings[enablepunycode]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enablepunycode]
                                                HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                                                HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[*]
                                                HKCU\software\microsoft\internet explorer\main[frametabwindow]
   Queries value:
   Oueries value:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main[frametabwindow]
                                                HKCU\software\microsoft\internet explorer\main[framemerging]
   Oueries value:
                                                HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
   Queries value:
                                                HKCU\software\microsoft\internet explorer\main[sessionmerging]
   Queries value:
   Queries value:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main[sessionmerging]
                                                HKCU\software\microsoft\internet explorer\main[admintabprocs]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main[admintabprocs]
                                                HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
   Queries value:
   Queries value:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main[tabprocgrowth]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main[navigationdelay]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
   Queries value:
HKLM \verb|\software\microsoft| windows \verb|\currentversion| policies \verb|\explorer[noproperties recyclebin]| \\
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
   Queries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[restrictedattributes]
   Oueries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsfordisplay]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsforparsing]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[quervforoverlav]
   Queries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[mapnetdriveverbs]
   Oueries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[queryforinfotip]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[hideinwebview]
   Oueries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[hideondesktopperuser]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
```

```
HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
   Oueries value:
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[nofilefolderjunction]
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[hasnavigationenum]
                                                      HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{871c5380-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus
   Oueries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ \ policies \ nonenum \ [\{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2
08002b30309d}1
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\inprocserver32[]
   Queries value:
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\shell
0xffff1
   Queries value:
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
   Queries value:
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
   Queries value:
                                                      HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
   Queries value:
                                                      HKLM\system\currentcontrolset\control\cmf\config[system]
                                                      HKCR\protocols\handler\res[clsid]
   Oueries value:
   Queries value:
                                                      HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[]
   Queries value:
                                                      HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                                                      HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[]
                                                     HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-
   Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
                                                     HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_legacy_dispparams[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
                                                     HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_object_caching[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                                                     HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_object_caching[*]
                                                      HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
   Oueries value:
   Queries value:
                                                      HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
91a2-7b624e0e7244]
   Queries value:
                                                      HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Queries value:
                                                      HKCU\software\microsoft\internet explorer\domstorage[totallimit]
                                                      HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                                      HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
   Oueries value:
                                                      HKLM\svstem\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Queries value:
                                                      HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
                                                      HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
   Queries value:
   Oueries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
                                                      HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_unc_savedfilecheck[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Queries value:
                                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
                                                      HKLM\software\policies\microsoft\internet
   Oueries value:
explorer\security[disablesecuritysettingscheck]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                                                      HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\2[flags]
                                                      HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[flags]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
   Oueries value:
                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Oueries value:
                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Oueries value:
                                                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                                                      HKLM\software\wow6432node\microsoft\internet
   Oueries value:
```

explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]

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

manager[safeprocesssearchmode]

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

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

Queries value:

settings[specialfolderscachesize]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

33be-4251-ba85-6007caedcf9d}[localredirectonlv] Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

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

folders[cache]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[category]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[name]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[parentfolder]

Oueries value:

c0e9-4171-908e-08a611b84ff6}[description]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

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

folders[cookies]

Queries value: HKCU\software\microsoft\internet explorer[no3dborder]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer[no3dborder] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[urlencoding]

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

settings[urlencoding]

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

explorer\main\featurecontrol\feature\_mime\_handling[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

explorer\main\featurecontrol\feature\_mime\_handling[\*]

Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]

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

 $explorer \verb|\main| featurecontrol| feature_restrict_res\_to\_lmz[83497c45d30bcb551f5f55f3f63b6fa1.exe]|$ 

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

explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz[\*]

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

explorer\main\featurecontrol\feature\_mime\_sniffing[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

 $\verb|explorer\main\featurecontrol\feature\_mime\_sniffing[*]|$ 

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

settings[istextplainhonored]

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

 $explorer \verb|\main| featurecontrol| feature_feeds[83497c45d30bcb551f5f55f3f63b6fa1.exe]|$ 

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

explorer\main\featurecontrol\feature\_feeds[\*]

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

settings[syncmode5]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

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

settings\5.0\cache[signature]

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

settings\5.0\cache\content[peruseritem]

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

settings\5.0\cache\content[peruseritem]

Queries value:

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

Oueries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$157091 $$[parentfolder] $$$ 

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\fifthm: $\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[local redirectonly]$$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fit bis 2785-66 ba-4fcf-9d55-7b8e7f157091 \fit bis 2785-9d6 ba-4fcf-9d55-7b8e7f157091 \fit bis 2785-9d6 ba-4fcf-9d55-7b8e7f157091 \fit bis 2785-9d6 \fit bis 27$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\ff1b32785-6fba-4fcf-9d55-7b8e7f157091\} [publishexpandedpath]$ 

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fill 1532785-65ba-4fcf-9d55-7b8e7f157091 \folder type id \folder \folder$ 

Queries value:

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

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ \ windows \ \ current version \ \ explorer \ \ shell \\$ 

folders[local appdata]

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folde$ 

Queries value:

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

Queries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{thm:local-state} $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[initfolderhandler]}$ 

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001[profileimagepath]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

 $Queries\ value: \\ HKLM\ software\ wow 6432 node\ microsoft\ windows\ current version\ internet$ 

settings\5.0\cache\cookies[peruseritem]

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\folder{29b685db-65f9-4cf6-a03a-e3ef65729f3d} [parentfolder]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{200} ab 685 db 65f9-4cf6-a03a-e3ef65729f3d\cite{200} [localized name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cal{lem:hklmsoftware} \end{substitute} folderdescriptions\cal{lem:hklmsoftware} folderdescriptions\cal{lem:hklmsoftware} \end{substitute} folderdescriptions\cal{lem:hklmsoftware} folderdescriptions\cal{lem:hklmsoftware$ 

Queries value:

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

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

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

folders[appdata]

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

settings\5.0\cache\cookies[cacheprefix]

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

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

Oueries value:

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

Queries value:

 $\label{limit} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[parsingname]} $$$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_explorer_local_ex$ 

```
b784-432e-a781-5a1130a75963}[precreate]
 Oueries value:
b784-432e-a781-5a1130a75963}[stream]
 Oueries value:
b784-432e-a781-5a1130a75963}[publishexpandedpath]
 Oueries value:
b784-432e-a781-5a1130a75963}[attributes]
 Oueries value:
b784-432e-a781-5a1130a75963}[foldertypeid]
 Oueries value:
b784-432e-a781-5a1130a75963}[initfolderhandler]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[history]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cachelimit]
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
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:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Oueries value:
settings[fromcachetimeout]
 Queries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[certificaterevocation]
```

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

```
settings[disablekeepalive]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablepassport]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries 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]
 Queries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                          HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enableautoproxyresultcache]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[displayscriptdownloadfailureui]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsservername]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsapiforcrack]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[utf8servernameres]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                          \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\current} internet
 Queries value:
settings[socketreceivebufferlength]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings[maxconnectionsper1 Oserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[serverinfotimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[disablentlmpreauth]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
                            HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
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\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                            HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablecachingofsslpages]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[perusercookies]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[leashlegacycookies]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[dialupuselansettings]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[wpadsearchalldomains]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[bypasshttpnocachecheck]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttptrace]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[nocheckautodialoverride]
  Queries value:
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Oueries value:
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[mimeexclusionlistforcache]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheentries]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnalwaysonpost]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[warnonzonecrossing]
  Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[warnonbadcertrecving]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpostredirect]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[alwaysdrainonredirect]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[tcpautotuning]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
```

- HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout]
  - Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[next\_catalog\_entry\_id]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001[packedcatalogitem]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006[packedcatalogitem]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[packedcatalogitem]
  Queries value:
  HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000009[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000002[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo]
  Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_library path] \\ Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[displaystring] Queries value:
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 0000000000003 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[storesserviceclassinfo]

Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[librarypath] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000004 \ [displaystring]$ Oueries value:

Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000004 [supported name space]]$ Oueries value:

Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[storesserviceclassinfo] Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath] Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[addressfamily] Oueries value:

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

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006[librarypath] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 0000000000006 \ [displaystring]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000006 [supported name space]]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 10000000000006 \ [storesservice class in fo]$ Oueries value:

Oueries value:

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

settings\wpad[wpadoverride]

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

settings[enableautodial]

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

settings[nonetautodial]

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

settings[globaluseroffline]

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

settings[badproxyexpirestime]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disablebranchcache]

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

Oueries value:

HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

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

explorer\main\featurecontrol\feature\_safe\_bindtoobject[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

explorer\main\featurecontrol\feature\_safe\_bindtoobject[\*]

Oueries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[] Oueries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]

Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

```
00aa00686f13}\inprocserver32[]
                          HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Oueries value:
00aa00686f13}\inprocserver32[threadingmodel]
                          HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\windows[dragscrollinset]
 Queries value:
                          HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
                         HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrollinterval]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer \verb|\main| featurecontrol| feature_restrict_filedownload[83497c45d30bcb551f5f55f3f63b6fa1.exe]|
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
                         HKCR\protocols\handler\about[clsid]
 Oueries value:
                          HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
 Queries value:
                          HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
 Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[]
 Oueries value:
                         HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                          HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[2106]
 Queries value:
                          HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
                          HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer[smartdithering]
 Queries value:
                          HKCU\software\microsoft\internet explorer[rtfconverterflags]
                          HKCU\software\microsoft\internet explorer\main[usecleartype]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[page_transitions]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
 Oueries value:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ internet\ explorer\+ main[anchor\ underline]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[css_compat]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[expand alt text]
                          HKCU\software\microsoft\internet explorer\main[display inline images]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[display inline videos]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet explorer\main[display
inline videos1
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[play_background_sounds]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[play_animations]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[print_background]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[use stylesheets]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[smoothscroll]
                          HKCU\software\microsoft\internet explorer\main[xmlhttp]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[show image placeholders]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[disable script debugger]
                          HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[move system caret]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[force offscreen
composition]
                          HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
 Queries value:
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[usethemes]
                          HKCU\software\microsoft\internet explorer\main[usehr]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[q300829]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[cleanup htcs]
                          HKCU\software\microsoft\internet explorer\main[xdomainrequest]
 Oueries value:
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main[xdomainrequest]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[domstorage]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\international[default_codepage]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\international[autodetect]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
                          HKCU\software\microsoft\internet explorer\settings[anchor color]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\settings[anchor color visited]
 Queries value:
                          HKCU\software\microsoft\internet explorer\settings[anchor color hover]
                          HKCU\software\microsoft\internet explorer\settings[always use my colors]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\settings[always use my font
size1
                          HKCU\software\microsoft\internet explorer\settings[always use my font
 Queries value:
face1
                          HKCU\software\microsoft\internet explorer\settings[disable visited
 Oueries value:
hyperlinks]
 Queries value:
                          HKCU\software\microsoft\internet explorer\settings[use anchor hover
color1
 Oueries value:
                          HKCU\software\microsoft\internet explorer\settings[miscflags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
```

 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ 

settings[disablecachingofsslpages] HKCU\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[disablecachingofsslpages] HKCU\software\microsoft\internet explorer\pagesetup[print\_background] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\codepage[950] Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsize] HKCU\software\microsoft\internet Oueries value: explorer\international\scripts\3[iefontsizeprivate] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iepropfontname] Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefixedfontname] HKCU\software\microsoft\internet explorer\international[acceptlanguage] Oueries value: Oueries value: HKLM\software\wow6432node\microsoft\internet explorer\version vector[vml] HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie] Queries value: Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version vector[windowsedition] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_zone\_elevation[83497c45d30bcb551f5f55f3f63b6fa1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation[\*] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_sslux[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_sslux[\*] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation[83497c45d30bcb551f5f55f3f63b6fa1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation[\*] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\0[2700] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0[2700] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_xssfilter[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature\_xssfilter[\*] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones[securitysafe] HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\low Oueries value: rights[protectedmodeoffforallzones] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[icon] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0[minlevel] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[currentlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[icon] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\1[minlevel] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\1[recommendedlevell Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[currentlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\1[2500] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[icon] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\2[minlevel] Queries value:  $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet$ settings\zones\2[recommendedlevell  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Queries value: settings\zones\2[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[2500] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\2[2500] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[icon] HKLM\software\wow6432node\microsoft\windows\currentversion\internet

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

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

Queries value:

Queries value:

settings\zones\3[minlevel]

settings\zones\3[recommendedlevel]

```
settings\zones\3[currentlevel]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2500]
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[2500]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[icon]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\4[minlevel]
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4[recommendedlevel]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\zones\4[currentlevel]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[2500]
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4[2500]
  Queries value:
                           HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
                           HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Oueries value:
                           HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                           HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\0[2106]
                           HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
  Queries value:
settings\zones\0[2106]
                           HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Oueries value:
                           HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:
                           HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Oueries value:
  Queries value:
                           HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[cointernetcombineiuricachesize]
  Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cointernetcombineiuricachesize]
                           HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
  Queries value:
settings[cointernetcombineiuricachesize]
  Queries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                           HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_shim_mshelp_combine[*]
                           HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
  Oueries value:
  Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 83497c 45d 30bc b 551f 5f 5f 3f 63b 6f a 1\_rasapi 32[filetracing mask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[enableconsoletracing]
  Oueries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32[consoletracing mask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasapi32[filedirectory]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
                           HKLM\software\microsoft\sqmclient\windows\disabledprocesses[b798a23b]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled sessions [machine throttling]
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Oueries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus tracing \setminus 83497 \\ c45d30bcb551f5f55f3f63b6fa1\_rasmancs[enablefile tracing]
  Queries value:
Queries value:
Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 83497c45d30bcb551f5f55f3f63b6fa1\_rasmancs[consoletracing mask]
  Oueries value:
HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus 83497c45d30bcb551f5f55f3f63b6fa1\_rasmancs [maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1_rasmancs[filedirectory]
  Queries value:
                           HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[proxysettingsperuser]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyserver]
```

```
Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[savedlegacysettings]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
 Queries value:
                        HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [allow unqualified query]
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [filter clusterip]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
 Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
```

```
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
 Oueries value:
                       HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnsquervtimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Queries value:
Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[dnsquickquervtimeouts]
 Queries value:
                       settings\url history[daystokeep]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\3[2700]
                       \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows + current version + internet
 Queries value:
settings\5.0\user agent[]
                       HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| internet
 Queries value:
settings\5.0\user agent[]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[compatible]
                       Queries value:
settings\5.0\user agent[compatible]
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[version]
                       HKCU\software\microsoft\windows\currentversion\internet settings[user
 Oueries value:
agent]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[platform]
                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[platform]
                       HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature maxconnectionsperserver[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
 Oueries value:
                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Oueries value:
                      HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsper1 0server[*1
 Oueries value:
                      HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
 Queries value:
                       HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
```

```
Oueries value:
                       HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enableutf8]
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[securityidiuricachesize]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[securityidiuricachesize]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[securityidiuricachesize]
                       HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[securityidiuricachesize]
                       HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_legacy_compression[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                      HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\[]
 Queries value:
                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
fd2b31b3eefd}\inprocserver32[inprocserver32]
 Queries value:
                       HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[]
                       Queries value:
fd2b31b3eefd}\inprocserver32[threadingmodel]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[1a10]
 Queries value:
                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
                       HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonintranet]
                       HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonintranet]
                       HKLM\system\currentcontrolset\services\winsock\setup
 Queries value:
migration\providers\tcpip6[winsock 2.0 provider id]
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
 Queries value:
                       HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                       HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
 Oueries value:
 Oueries value:
                       HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                       HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
 Queries value:
f4ceaaf59cfc}\inprocserver32[]
 Queries value:
                       HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                       HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Oueries value:
 Oueries value:
Queries value:
e1e01c1f69b5}[searchlist]
                       HKCU\software\microsoft\internet explorer\recovery[autorecover]
 Oueries value:
 Queries value:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2000]
 Queries value:
e1e01c1f69b5}[enabledhcp]
                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\0[2000]
 Oueries value:
                       HKLM\software\wow6432node\microsoft\internet explorer\feed
discovery[sound]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationenabled]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[domain]
```

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}{dhcpdomain1

Oueries value:

Queries value:

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

Queries value: HKCU\software\microsoft\ftp[use web based ftp]

Oueries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM \ system \ `current controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee342-7039-11de-9d20-806e6f6e6963\} \ [enabled \ hcp]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \end{20-806e6f6e6963} \ [registration enabled]$ 

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [register adapter name]$ 

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \ system \ `current controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee342-7039-11de-9d20-806e6f6e6963\} \ [dhcpdomain]$ 

Queries value:

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

Queries value:

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

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \system \current control set \services \tcpip\parameters \interfaces \end{4.846} and \system \e$ 

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [disable dynamic update]$ 

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

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

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

settings\zones\3[{a8a88c49-5eb2-4990-a1a2-0876022c854f}]

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

settings[privacyadvanced]

Queries value: HKCR\mime\database\content type\text/html[extension]

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

 $explorer \verb|\main| featurecontrol| feature\_subdownload\_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]|$ 

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

explorer\main\featurecontrol\feature\_subdownload\_lockdown[\*]

```
Queries value:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings[privdiscuishown]
                                               HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\3[1400]
                                               HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_block_lmz_script[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Oueries value:
                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[*]
   Queries value:
                                               HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid[]
                                               HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
   Oueries value:
                                               HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
   Oueries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
   Queries value:
                                               HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[]
   Queries value:
                                               HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
                                               HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[1201]
   Queries value:
                                               HKLM\software\microsoft\rpc\extensions[ndroleextdll]
   Oueries value:
                                               HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
   Queries value:
                                               HKLM\software\microsoft\ole[defaultaccesspermission]
   Queries value:
                                               HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Oueries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
   Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \
provider[image path]
                                               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Oueries value:
   Queries value:
                                               HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
                                               HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
   Oueries value:
   Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds] \\
   Queries value:
                                               HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                               HKLM\software\microsoft\cryptography[machineguid]
   Oueries value:
                                               HKCR\wow6432node\interface\{00000134-0000-0000-c000-
   Queries value:
00000000046}\proxystubclsid32[]
                                               HKLM\software\microsoft\rpc\extensions[remoterpcdll]
   Oueries value:
                                               HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_use_windowedselectcontrol[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Queries value:
                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
   Oueries value:
                                               HKCU\software\microsoft\windows script\settings[iitdebug]
                                               HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}[]
   Queries value:
                                               HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
   Oueries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                                               HKCR \setminus 6432 \\ node \\ clsid \\ \{3050f391-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[]
                                               HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
   Oueries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
                                               HKLM\software\wow6432node\microsoft\internet explorer\abouturls[blank]
   Oueries value:
                                               HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                                               HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
   Queries value:
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7[*]
   Queries value:
                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[83497c45d30bcb551f5f55f3f63b6fa1.exe]
   Oueries value:
                                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature block lmz img[*]
                                               HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\language| pack \verb| datastore_v1.0[disable]|
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                                               HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane1]
                                               HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
                                               HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
   Queries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                               HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
   Oueries value:
                                               HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
   Oueries value:
                                               HKLM\software\microsoft\windows
```

nt\currentversion\languagepack\surrogatefallback[plane10]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane11] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane12] HKLM\software\microsoft\windows Oueries value:  $\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|$ Queries value: HKLM\software\microsoft\windows  $\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane15] HKLM\software\microsoft\windows Oueries value:  $\verb|nt\currentversion\languagepack\surrogatefallback[plane16]|$ 

Queries value: HKCR\mime\database\content type\image/jpeg[extension]

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

explorer\main[maxrenderline]

Queries value: HKCU\software\microsoft\internet

explorer\services[selectionactivitybuttondisable]

Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]

Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 83497 c 45 d 30 b c b 551 f 5 f 5 f 3 f 63 b 6 f a 1\_rasapi 32 [enable file tracing] \\ Sets / Creates value:$ 

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32[enableconsoletracing] Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32[filetracingmask]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32[consoletracingmask]
 Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32[maxfilesize]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasapi32[filedirectory]
Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ tracing \ 83497 c 45 d 30 b c b 551 f 5 f 5 f 3 f 63 b 6 f a 1\_rasmancs \ [enable file tracing] \\ Sets / Creates \ value:$ 

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasmancs[enableconsoletracing]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasmancs[filetracingmask]
 Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasmancs[consoletracingmask]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\83497c45d30bcb551f5f55f3f63b6fa1\_rasmancs[maxfilesize]
Sets/Creates value:

 $HKLM \backslash software \backslash wow6432 node \backslash microsoft \backslash tracing \backslash 83497 c45 d30 bcb551 f5f55f3f63 b6fa1\_rasmancs [filedirectory]$ 

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

settings\zonemap[uncasintranet]

 $\label{thm:condition} \mbox{Value changes:} \qquad \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\internet}}$ 

settings\zonemap[autodetect]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]