Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 11, Task ID: 41

Task ID: 41 Risk Level:

Date Processed: 2016-04-28 12:46:59 (UTC)

Processing Time: 60.49 seconds Virtual Environment: IntelliVM

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

Sample ID: Type: basic admin Owner:

83497c45d30bcb551f5f55f3f63b6fa1 Label:

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

PE32:win32:gui File Type: File Size: 892928 bytes

83497c45d30bcb551f5f55f3f63b6fa1 MD5:

40932ac88b750f1f3077f2e50d9184de1c3b4914e92ceb64cfc4638c3d91ee14 SHA256:

Description: None

Pattern Matching Results

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

\Sessions\1\BaseNamedObjects\DBWinMutex Creates mutex

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

\Sessions\1\BaseNamedObjects\!IECompat!Mutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex

File System Events

C:\Users\Admin Creates

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

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

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

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

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

Files\Content.IE5\T2095MVJ\104[1]

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

Files\Content.IE5\LXTB75Y0\property_front[1].htm

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Creates Files\Content.IE5\P8S8Q01R\property_front[1].htm

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

Files\Content.IE5\LXTB75Y0\JMX.Frame.Common[1].js

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

Files\Content.IE5\LXTB75Y0\jquery-1.4.2.min[1].js

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

Files\Content.IE5\LXTB75Y0\JMX_FormValidator[1].js C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\41101FRQ\JMX_AjaxControl[1].js

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

Files\Content.IE5\T2095MVJ\client_ending[1].htm Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\P8S8Q01R\SRO-ending[1].jpg

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

Files\Content.IE5\P8S8Q01R\btn_facebook[1].jpg

C:\Windows\Prefetch\83497C45D30BCB551F5F55F3F63B6-CCFC2B0F.pf Opens:

Opens: C:\Windows

Opens:

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

Opens: C:\Windows\SysWOW64

C:\Windows\SysWOW64\apphelp.dll Opens: Opens: C:\Windows\Temp\83497c45d30bcb551f5f55f3f63b6fa1.exe

C:\Windows\SysWOW64\ntdll.dll Opens: Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: C:\Windows\apppatch\sysmain.sdb

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

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954

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

C:\Windows\SysWOW64\winspool.drv

```
C:\Windows\SysWOW64\oledlg.dll
                         C:\Windows\SysWOW64\sechost.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\combase.dll
 Opens:
                         C:\Windows\SysWOW64\SHCore.dll
 Opens:
                         C:\Windows\SysWOW64\gdi32.dll
                         C:\Windows\SysWOW64\user32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\msvcrt.dll
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
                         C:\Windows\SysWOW64\bcryptprimitives.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptbase.dll
 Opens:
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
                         C:\Windows\SysWOW64\rpcrt4.dll
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
                         C:\Windows\SysWOW64\comdlg32.dll
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
                         C:\Windows\SysWOW64\oleaut32.dll
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\Windows\SysWOW64\msctf.dll
 Opens:
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.2.Manifest
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.3.Manifest
 Opens:
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.Config
 Opens:
                         C:\windows\temp\83497c45d30bcb551f5f55f3f63b6fa1.exe.1000.Manifest
 Opens:
                         C:\Windows\Fonts\tahoma.ttf
 Opens:
                         C:\Windows\winhlp32.exe
 Opens:
                         C:\Windows\SysWOW64\clbcatq.dll
 Opens:
                         C:\Windows\SysWOW64\ieframe.dll
 Opens:
                         C:\Windows\SysWOW64\iertutil.dll
 Opens:
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
                         C:\Windows\SysWOW64\secur32.dll
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
                         {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
Files\counters.dat
 Opens:
                         C:\Windows\SysWOW64\nsi.dll
                         C:\Windows\SysWOW64\ws2_32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winhttp.dll
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
                         C:\Windows\SysWOW64\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mshtml.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dwmapi.dll
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\urlmon.dll.mui
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\Windows\SysWOW64\mlang.dll
 Opens:
                         C:\Windows\SysWOW64\propsys.dll
                         C:\Windows\SysWOW64\msimtf.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\msls31.dll
 Opens:
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
                         C:\Windows\SysWOW64\powrprof.dll
 Opens:
                         C:\Windows\SysWOW64\dxgi.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
                         C:\Windows\SysWOW64\d2d1.dll
 Opens:
                         C:\Windows\SysWOW64\DWrite.dll
 Opens:
                         C:\Windows\SysWOW64\d3d11.dll
 Opens:
                         C:\Windows\System32\Drivers\etc\hosts
                         C:\Windows\SysWOW64\d3d10warp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.DLL
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LXTB75Y0\property_front[1].htm
 Opens:
                         C:\Windows\SysWOW64\winmm.dll
 Opens:
                         C:\Windows\SysWOW64\winmmbase.dll
                         \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
 Opens:
Files\Content.IE5\P8S8Q01R\property_front[1].htm
                         C:\Windows\SysWOW64\sxs.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\stdole2.tlb
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LXTB75Y0\JMX.Frame.Common[1].js
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\LXTB75Y0\jquery-1.4.2.min[1].js
```

controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll

Opens:

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

Files\Content.IE5\LXTB75Y0\JMX_FormValidator[1].js

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

Files\Content.IE5\41101FRQ\JMX_AjaxControl[1].js

Opens: C:\Windows\SysWOW64\jscript9.dll

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

Files\Content.IE5\T2095MVJ\client_ending[1].htm

C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT Opens:

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

Opens: C:\Windows\Fonts\micross.ttf C:\Windows\Fonts\times.ttf Opens:

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

Opens: C:\Windows\SysWOW64\msxml6.dll Opens: C:\Windows\SysWOW64\msxml6r.dll

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

Files\Content.IE5\T2095MVJ\104[1]

Writes to:

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

Files\Content.IE5\LXTB75Y0\property_front[1].htm

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

Files\Content.IE5\P8S8Q01R\property front[1].htm

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

Files\Content.IE5\LXTB75Y0\JMX.Frame.Common[1].js C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\LXTB75Y0\jquery-1.4.2.min[1].js

Writes to:

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet $Files \verb|\Content.IE5\LXTB75Y0\JMX_FormValidator[1].js|$

Writes to:

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\41101FRQ\JMX_AjaxControl[1].js

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

Files\Content.IE5\T2095MVJ\client_ending[1].htm

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

Files\Content.IE5\P8S8Q01R\SRO-ending[1].jpg

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

Files\Content.IE5\P8S8Q01R\btn_facebook[1].jpg

C:\Windows\System32\Drivers\etc\hosts Reads from: Reads from: C:\Windows\SysWOW64\ieframe.dll Reads from: C:\Windows\SysWOW64\stdole2.tlb

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

Files\Content.IE5\LXTB75Y0\jquery-1.4.2.min[1].js

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

Files\Content.IE5\LXTB75Y0\JMX_FormValidator[1].js

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

Files\Content.IE5\41101FRQ\JMX_AjaxControl[1].js

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

Files\Content.IE5\LXTB75Y0\JMX.Frame.Common[1].js

Network Events

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

Connects to: 127.0.0.1:50622 Connects to: 222.111.176.232:80 Connects to: 121.128.133.12:80 Connects to: 119.31.253.194:80 Sends data to: 0.0.0.0:53 Sends data to: 127.0.0.1:50622

Sends data to: file.joymax.com:80 (222.111.176.232) Sends data to: silkroadcp.joymax.com:80 (121.128.133.12) Sends data to: img.joymax.com.gccdn.net:80 (119.31.253.194)

Receives data from: 0.0.0.0:53 Receives data from: 127.0.0.1:50622

Receives data from: file.joymax.com:80 (222.111.176.232) Receives data from: silkroadcp.joymax.com:80 (121.128.133.12) 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

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

settings\zonemap\

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

settings\connections

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Creates kev: HKCU\software\microsoft\internet explorer\main

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

settings\p3p\history

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

settings\zonemap[proxybypass]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[intranetname]

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]

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

settings[autodetect]

Opens key: HKLM\software\microsoft\wow64

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

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

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\disable8and16bitmitigation
 Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key:

Opens key:

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

HKLM\software\microsoft\windows nt\currentversion\image file execution

execution options

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

Opens key: HKLM\so nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

Opens key: HKLM\

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

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

Opens key: HKLM\system\currentcontrol\lsa

Opens key:

 ${\tt HKLM \ } system \verb|\ current control set \verb|\ policies \verb|\ microsoft \verb|\ cryptography \verb|\ configuration \\$

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

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

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

Opens key: HKCU\software\classes\

Opens key: $\begin{tabular}{ll} HKCU\software\classes\ww6432node\clsid \\ Opens key: \\ HKCR\ww6432node\clsid \\ \end{tabular}$

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

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

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

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

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups

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

Opens key: HKLM\software\microsoft\com3

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

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{8856f961-340a-11d0-a96b-

```
00c04fd705a2}
                                                                            HKCR\activatableclasses\clsid
     Opens kev:
                                                                            HKCR\activatableclasses\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
     Opens key:
                                                                            HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
     Opens key:
00c04fd705a2}
     Opens key:
                                                                            HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{8856f961 - 340a - 11d0 - a96b - 00c04fd705a2\}
                                                                            HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-12d1\} \\ \cap (3856f961-340a-11d0-a96b-12d1) 
     Opens key:
00c04fd705a2}\treatas
     Opens key:
                                                                            \label{locality} HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
                                                                            HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
     Opens key:
00c04fd705a2}\inprocserver32
     Opens key:
                                                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
 00c04fd705a2}\inprocserver32
                                                                           HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
     Opens key:
00c04fd705a2}\inprochandler32
     Opens key:
                                                                           HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
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
     Opens key:
                                                                           HKLM\system\currentcontrolset\control\nls\sorting\ids
     Opens kev:
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
                                                                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearings}} \ \ \mbox{\tt microsoft\windows\currentversion\linearings}} \ \mbox{\tt microsoft\windows\currentversion\linearings}} \ \ \mbox{\tt microsoft\windows\currentversion\linearings}} \ \mbox{\tt microsoft\windows\currentversion\windows\currentversion\linearings}} \ \mbox{\tt microsoft\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\currentversion\windows\windows\windows\windows\currentversion\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
     Opens key:
     Opens key:
                                                                            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings
                                                                           HKLM\software\wow6432node\policies\microsoft\internet
     Opens key:
 explorer\main\featurecontrol
     Opens key:
                                                                           HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
                                                                           HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
     Opens key:
     Opens key:
                                                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
                                                                           HKCU\software\microsoft\internet explorer\main\featurecontrol
     Opens key:
     Opens key:
                                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
     Opens key:
                                                                           HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
     Opens kev:
                                                                           HKCU\software\microsoft\internet explorer\main
     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:
                                                                           \label{lem:hkcu} \mbox{HKCU\software\policies\mbox{\sc microsoft\internet explorer\mbox{\sc main}} \\
     Opens key:
                                                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol\msinternal metro allow tpg zero
     Opens key:
                                                                           HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\msinternal_metro_allow_tpg_zero
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
                                                                            HKLM\software\microsoft\windows\currentversion\policies\explorer
     Opens key:
     Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 83497c45d30bcb551f5f55f3f63b6fa1.exe
     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
                                                                            \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \label{thm:local_hammon} Software \end{tabular} in the local hammon \begin{tabular}{ll} HKCU \end{tabular} is the local hammon \begin{tabular}{ll} HKCU \end{tabular} in the local hammon \begin{tabular}{ll} HKCU \end{t
     Opens key:
     Opens key:
HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| windows \verb|\currentversion\\| policies\\| none numerous and the properties of the propertie
     Opens key:
                                                                            HKLM\software\microsoft\windows\currentversion\policies\nonenum
     Opens key:
                                                                           HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
     Opens key:
                                                                            HKLM\software\wow6432node\microsoft\windows\currentversion\shell
extensions\blocked
     Opens key:
                                                                            HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
     Opens key:
                                                                            HKLM\system\currentcontrolset\control\session manager\appcompatibility
     Opens key:
                                                                            HKLM\software\wow6432node\policies\microsoft\windows\appcompat
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows\appcompat
     Opens key:
                                                                            \label{thm:constraint} \begin{tabular}{ll} HKCU \software \begin{tabular}{ll} windows \current version \shell extensions \cached \end{tabular}
     Opens kev:
                                                                            HKLM\software\microsoft\windowsruntime\clsid\{871c5380-42a0-1069-a2ea-
```

HKCR\activatableclasses\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

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

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

Opens key: 08002b30309d}\treatas

08002b30309d}

Opens key: Opens key:

08002b30309d} Opens key:

Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32 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 Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{871c5380-microsoft) \ moreover \ m$ 42a0-1069-a2ea-08002b30309d} Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_iedde_register_protocol Opens key: HKLM\software\wow6432node\microsoft\rpc Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\$ Opens key: HKLM\system\setup Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc Opens kev: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions$ Opens key: 33be-4251-ba85-6007caedcf9d} Opens key: 33be-4251-ba85-6007caedcf9d}\propertybag Opens key: HKCU\software\microsoft\windows\currentversion\explorer $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session in fo \setminus 1$ Opens kev: Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus explorer \setminus session in folders$ Opens key: HKU\ Opens key: HKU\.default Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\profilelist HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_http_username_password_disable HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_http_username_password_disable HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\retry headeronlypost onconnectionreset Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature mime handling HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet$ Opens key: explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy 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 Opens key: HKCU\software\microsoft\internet 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 key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
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: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet

```
HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 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 key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                       HKCU\software\microsoft\internet
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
                      HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
 Opens key:
                       HKLM\software\wow6432node\policies
 Opens key:
                       HKCU\software\policies
                       HKCU\software
 Opens key:
 Opens key:
                       HKLM\software\wow6432node
 Opens key:
                       HKLM\software\wow6432node\policies\microsoft\internet explorer
 Opens key:
                       HKLM\software\policies\microsoft\internet explorer
 Opens key:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
                       Opens key:
settings\5.0\cache
                       HKCU\software\microsoft\internet
 Opens key:
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
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                       HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\14993e33
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens kev:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries
 Opens kev:
Opens key:
Opens kev:
```

explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149

Opens key:

Opens kev:

Opens kev:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens kev:

Opens key:

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens key:

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

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

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

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

migration\providers\tcpip6

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

explorer\browseremulation

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

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

HKCR\protocols\name-space handler Opens key:

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

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

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

Opens key: HKCR\protocols\name-space handler*

HKCU\software\classes\protocols\handler\res Opens kev:

Opens key: HKCR\protocols\handler\res

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}

HKCR\activatableclasses\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{3050f3bc-98b5-11cf-bb82-11cf-$ 00aa00bdce0b}

Opens key:

HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\treatas

HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprocserv er32

Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens key:

00aa00bdce0b}\inprochandler

HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprochandler

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature gpu rendering

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

explorer\main\featurecontrol\feature_gpu_rendering

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120 HKLM\software\wow6432node\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120

Opens key: HKCU\software\microsoft\internet

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 kev:
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                         HKCU\software\microsoft\internet
 Opens key:
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 key:
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
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_object_caching
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_download_initiator_http_header
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_download_initiator_http_header
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature mobile customizations
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_mobile_customizations
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_high_resolution_aware
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_high_resolution_aware
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_force_disable_untrustedprotocol
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_force_disable_untrustedprotocol
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_weboc_omnavigator_implementation
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_weboc_omnavigator_implementation
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_security_thunks
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_security_thunks
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_deferred_image_download
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_deferred_image_download
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_lazy_image_decoding
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
```

```
explorer\main\featurecontrol\feature_lazy_image_decoding
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_intranet_css_mime_mismatch
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_intranet_css_mime_mismatch
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_clipchildren_optimization
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_clipchildren_optimization
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_larger_hit_test
 Opens key:
                         HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_enable_larger_hit_test
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_legacy_jscript
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_legacy_jscript
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mobile_viewport_width_restrictions
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mobile_viewport_width_restrictions
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_xdomainrequest
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xdomainrequest
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_websocket
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_websocket
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_uniscribe
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_uniscribe
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_ninput_legacymode
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_ninput_legacymode
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_hang_recovery_touch_mitigation
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_hang_recovery_touch_mitigation
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_paint_inside_wmpaint
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_paint_inside_wmpaint
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_software_filter_rendering
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_software_filter_rendering
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_spellchecking
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_spellchecking
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_structure_node_child_count
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_structure_node_child_count
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_tune_hang_recovery_touch_mitigation
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_tune_hang_recovery_touch_mitigation
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_force_natural_text_metrics
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_force_natural_text_metrics
                         HKCU\software\microsoft\windows nt\currentversion\windows
 Opens kev:
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
 Opens key:
                         paths\outlook.exe
                         \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} soft \end{tabular} windows \end{tabular} current version \end{tabular} paths \end{tabular} outlook. exe
 Opens key:
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility
                         HKLM\software\wow6432node\policies\microsoft\internet
 Opens key:
explorer\domstorage
```

HKLM\software\policies\microsoft\internet explorer\domstorage

HKCU\software\policies\microsoft\internet explorer\domstorage

Opens key: Opens key:

HKCU\software\microsoft\internet explorer\domstorage Opens key: Opens key: HKLM\software\wow6432node\microsoft\internet explorer\domstorage HKCU\software\policies\microsoft\internet explorer\persistence Opens kev: Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\persistence Opens key: HKLM\software\policies\microsoft\internet explorer\persistence HKLM\software\wow6432node\microsoft\internet explorer\mediatypeclass Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\accepted documents Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings Opens key: HKLM\software\microsoft\windows\currentversion\policies\ratings Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet$ 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\zonemap\ranges\ Opens key: HKCU\zonemap\ranges\ 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: Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_browser_compatdata HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_browser_compatdata 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 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615 Opens key: HKLM\software\policies\microsoft\internet explorer\security HKCU\software\microsoft\windows\currentversion\internet settings\zones\ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet settings \setminus zones \setminus 3$ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones Opens key: settings\zones\ Opens key:

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

Settings\zones\u Opens key:

```
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
 Opens kev:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens key:
                            HKCU\software\microsoft\windows\currentversion\internet
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 key:
                            \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\zones\2
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\3
 Opens key:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\4
  Opens key:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                           HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                           HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer \verb|\main\featurecontrol\feature\_localmachine\_lockdown|
  Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet
settings\lockdown_zones\
                            HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones
 Opens key:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\
                            HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown zones\0
 Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown zones\0
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\1
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Opens key:
settings\lockdown zones\2
 Opens key:
settings\lockdown_zones\2
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
                            HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
 Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\3
  Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
 Opens key:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\lockdown_zones\4
 Opens key:
settings\lockdown zones\4
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                           \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Opens kev:
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
                                  HKCR\protocols\handler\c
  Opens key:
                                  HKCU\software\microsoft\internet
  Opens kev:
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\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens kev:
c0e9-4171-908e-08a611b84ff6}
  Opens key:
c0e9-4171-908e-08a611b84ff6}\propertybag
  Opens kev:
                                  HKCU\software\microsoft\internet explorer
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet explorer
  Opens key:
                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_olealias_gwnd
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_olealias_gwnd
                                  HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_topmost_gwnd
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_topmost_gwnd
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_aligned_timers
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_aligned_timers
                                  HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_restrict_res_to_lmz
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_restrict_res_to_lmz
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_load_shdoclc_resources
                                  HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_load_shdoclc_resources
                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:
                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                                  HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_feeds
                                  HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_feeds
  Opens key:
                                  HKCU \setminus software \setminus classes \setminus protocols \setminus filter \setminus text/html
  Opens key:
                                  HKCR\protocols\filter\text/html
  Opens kev:
                                  HKCU\software\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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}
  Opens kev:
6fba-4fcf-9d55-7b8e7f157091}\propertybag
0e22-4760-9afe-ea3317b67173}
  Opens key:
0e22-4760-9afe-ea3317b67173}
                                  HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
  Opens key:
                                  HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
  Opens kev:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ folde
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
  Opens kev:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
```

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d9dc8a1b-d$

b784-432e-a781-5a1130a75963} Opens key:

Opens key:

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

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

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

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

explorer\main\featurecontrol\feature_protocol_lockdown

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

settings\zones\0

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 11$

00aa00686f13}

Opens key: $HKCR \land activatable classes \land clsid \land \{25336920-03f9-11cf-8fd0-00aa00686f13\}$ Opens key: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}

Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13} HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key:

00aa00686f13}\treatas

Opens key: $HKCR\wow6432 node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treat as$ Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 11cf$

00aa00686f13}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprocserver32

Opens kev: HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\inprochandler32

Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 11cf$

00aa00686f13}\inprochandler

HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-Opens key:

00aa00686f13}\inprochandler

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

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

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

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\security\floppy

access

Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof detection

Opens key:

addrbar spoof detection Opens key: HKCU\software\classes\protocols\name-space handler\about\

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

Opens key: HKCR\protocols\handler\about

 $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{3050f406-98b5-11cf-bb82-11c$ Opens key:

00aa00bdce0b}

HKCR\activatableclasses\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens kev: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{3050 \\ f406 - 98 \\ b5 - 11 \\ cf - bb \\ 82 - bb \\ 11 \\ cf - bb \\ 82 - bb \\ 12 \\ cf - bb \\ 12 \\ cf - bb \\ 13 \\ cf - bb \\ 13 \\ cf - bb \\ 14 \\ cf -$ Opens key: 00aa00bdce0b}

HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\treatas

Opens kev: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{3050f406 - 98b5 - 11cf - bb82 - bb82$ Opens key: 00aa00bdce0b}\inprochandler32

Opens key:

HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprochandler

HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprochandler

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

settings\zones\3

Opens kev: 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

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\zoom Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_weboc_document_zoom

Opens key:

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

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

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

```
explorer\main\featurecontrol\feature_allow_highfreq_timers
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_highfreq_timers
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
 Opens key:
                         HKCR\wow6432 node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\\progid
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens kev:
 Opens key:
explorer\international\scripts
```

HKLM\software\wow6432node\microsoft\internet

HKCU\software\microsoft\internet explorer\international $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus internet$

Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts Opens key: HKCU\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\wow6432node\policies\microsoft\internet explorer\settings

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

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

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

Opens key: HKCU\software\microsoft\internet explorer\text scaling HKCU\software\microsoft\internet explorer\viewport Opens key: Opens key: HKCU\software\microsoft\internet explorer\larger hit test Opens key: HKCU\software\microsoft\internet explorer\script

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet$ Opens kev:

explorer\advancedoptions\disambiguation

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

Opens key: HKCU\software\microsoft\windows\currentversion\policies Opens key: HKCU\software\microsoft\internet explorer\pagesetup Opens key: HKCU\software\microsoft\internet explorer\menuext Opens key: HKLM\system\currentcontrolset\control\nls\codepage

Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3

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

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

explorer\main\featurecontrol\feature_restrict_filedownload

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

Opens key:

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

HKLM\software\microsoft\windowsruntime\clsid\{e569bde7-a8dc-47f3-893f-Opens key:

fd2b31b3eefd}

Opens key: HKCR\activatableclasses\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd} $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - a8dc - 47f3 - 800f - 800f$ Opens key: fd2b31b3eefd}

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}

Opens key:

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e569bde7 - a8dc - 47f3 - 893f - a8dc - 47f3 - 800f - a8dc - 47f3 - a8dc - a8dc$ Opens key: fd2b31b3eefd}\treatas HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas Opens key:

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

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

fd2b31b3eefd}\inprocserver32 Opens key:

fd2b31b3eefd}\inprocserver32

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

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\version vector

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

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

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

HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature disable navigation sounds

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

explorer\iedevtools\options

HKLM\software\policies\microsoft\internet explorer\iedevtools\options Opens kev: HKCU\software\policies\microsoft\internet explorer\iedevtools\options Opens key:

Opens key: HKCU\software\microsoft\internet explorer\iedevtools\options

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\iedevtools\options

Opens key:

 $HKCU \ software \ microsoft \ windows \ shell \ associations \ mimeassociations \ text/xml \ userchoice$ HKCU\software\classes\mime\database\content type\text/xml Opens kev:

Opens key: HKCR\mime\database\content type\text/xml Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_xssfilter

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

explorer\main\featurecontrol\feature_xssfilter

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

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

explorer\main\featurecontrol\feature_process_xml_as_html

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

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

Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\low rights

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\low rights
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: 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 key:

 $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic$

provider

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

Opens key: HKLM\software\microsoft\cryptography

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

Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-

000000000046}

 $000000000046 \} \verb|\proxystubclsid32|$

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

00000000046}\proxystubclsid32

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

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

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

settings\zones\1

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

settings\zones\2

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

settings\zones\4
Opens kev:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus significant in the compatibility \setminus 83497c45d30bcb551f5f55f3f63b6fa1.exe$

Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
Opens key: HKCU\software\microsoft\internet

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

Opens key: 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

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

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

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

Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\wow6432node\policies\microsoft\windows

nt\dnsclient\dnspolicyconfig

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

Opens key:

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

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

settings\winhttp

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

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

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

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

settings\url history

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

settings\url history

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

history

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

settings\url history

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

Opens key: HKCR\protocols\name-space handler\http

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

settings\5.0\user agent

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

settings\5.0\user agent

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

settings\user agent

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

settings\user agent

Opens key:

settings\5.0\user agent\pre platform

 $\label{thm:condition} \parbox{$HKCU$\software\microsoft\windows\currentversion\internet} \\$ Opens key:

settings\5.0\user agent\pre platform

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

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \begin{tabul$ 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

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

explorer\main\featurecontrol\feature_maxconnectionsperserver Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server

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

migration\providers\tcpip

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

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

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

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

explorer\main\featurecontrol\feature_urlmon_iqda_size

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

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

explorer\browserstorage\appcache

Opens key: HKCU\software\microsoft\internet explorer\browserstorage\appcache

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

explorer\browserstorage\appcache

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

Opens key: HKCU\software\microsoft\internet explorer\browseremulation Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

settings\

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

settings\

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

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

explorer\restrictions

Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions HKCU\software\policies\microsoft\internet explorer\restrictions Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d2$ Opens key:

f4ceaaf59cfc}

Opens key: HKCR\activatableclasses\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc} Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d278$

f4ceaaf59cfc}

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

f4ceaaf59cfc}\treatas

Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d278$ Opens key:

f4ceaaf59cfc}\inprocserver32

HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-Opens kev:

f4ceaaf59cfc}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{50d5107a - d278 - 4871 - 8989 - d278 - d278$ Opens key:

f4ceaaf59cfc}\inprochandler32

HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-Opens key:

f4ceaaf59cfc}\inprochandler32

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

f4ceaaf59cfc}\inprochandler

HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-Opens key:

f4ceaaf59cfc}\inprochandler

Opens key:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens kev:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

HKCU\software\microsoft\direct3d Opens key: Opens key: HKLM\software\wow6432node\microsoft\direct3d HKLM\software\wow6432node\microsoft\direct3d\drivers Opens kev: Opens key: HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist Opens key: HKCU\software\microsoft\dxgi Opens key: HKLM\software\wow6432node\microsoft\dxgi Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9} HKCU\software\policies\microsoft\internet explorer\control panel Opens key: Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963} Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces Opens key: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-be12e1de57-d6fa-11e1-be12$ 806e6f6e6963} Opens key: 25b8d56dd1d8} Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-8a6dc56e0da9} Opens key: 55779daa70e9} Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage HKLM\system\currentcontrolset\services\fontcache\parameters Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\control\graphicsdrivers\scheduler HKCU\software\microsoft\internet explorer\gpu Opens key: Opens key: HKCU\eudc\ Opens key: HKCU\eudc\1252 HKLM\software\policies\microsoft\internet explorer\recovery Opens key: Opens key: HKCU\software\microsoft\internet explorer\recovery Opens key: HKCU\software\microsoft\internet explorer\feed discovery $\label{lem:hklm} \verb+KLM\software\wow6432node\microsoft\internet\ explorer\feed\ discovery$ Opens key: Opens key: HKCU\software\microsoft\ftp Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_paint_for_page_enter HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_block_paint_for_page_enter $\label{lem:hklm} \verb+ HKLM \software \policies \microsoft \normalisation explorer \normalisation explorer \normalisation and the lemma \normalisation of \normalisation explorer \normalisation \normalisati$ Opens key: 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 HKCU\software\policies\microsoft\internet Opens key: explorer\infodelivery\restrictions 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\appevents\schemes\ Opens key: HKCU\appevents\schemes\apps\explorer\navigating\.current Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p\history\joymax.com Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_subdownload_lockdown Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_use_builtin_accept_headers HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature mime use builtin accept headers HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup

Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup

 $Opens\ key: \\ \hspace*{0.5cm} \mathsf{HKCU} \land \mathsf{appevents} \land \mathsf{schemes} \land \mathsf{apps} \land \mathsf{explorer} \land \mathsf{ctivating} document \land \mathsf{current} \\$

Opens key: HKCU\software\classes\typelib

Opens key: HKCR\typelib

Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}

Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}

Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1

 $HKCR \typelib \end{tab22} ac0-30c1-11cf-a7eb-0000c05bae0b \label{tab22} 1.1$ Opens key: Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0 HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0 Opens key: Opens kev: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32 $HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32$ Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046} Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046} Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-0000-00000000046}\2.0 Opens key: Opens key: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0 HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0 Opens key: Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32 HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32 Opens kev: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_block_lmz_script Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script Opens key: HKLM\software\microsoft\windowsruntime\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755} HKCR\activatableclasses\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755} HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Off4dc41e755}\treatas HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}\treatas Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{16d51579 - a30b - 4c8b - a276 - a276$ Off4dc41e755}\inprocserver32 HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens key: Off4dc41e755}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens kev: Off4dc41e755}\inprochandler32 HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens key: Off4dc41e755}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Off4dc41e755}\inprochandler HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-Opens kev: Off4dc41e755}\inprochandler HKCU\software\microsoft\internet explorer\jscript9 Opens kev: HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547 Opens key: HKLM\software\microsoft\windowsruntime\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f} HKCR\activatableclasses\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f} Opens key: Opens key: 8bc445b9828f} Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f} Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\treatas HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\treatas Opens kev: Opens key: 8bc445b9828f}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprocserver32 Opens key: 8bc445b9828f}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler Opens key: HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}\inprochandler HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert HKLM\software\wow6432node\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
 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:
                                                                HKLM\software\microsoft\windowsruntime\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}
    Opens key:
                                                                HKCR\activatableclasses\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
    Opens kev:
                                                                HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}
                                                                HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
    Opens key:
    Opens key:
                                                                HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                                                HKCR\wow6432 node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\treat as
    Opens key:
    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 kev:
                                                                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
                                                                HKCU\software\classes\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
    Opens kev:
00aa00bdce0b}\progid
    Opens key:
                                                                HKCR\wow6432 node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\ \ progid
                                                                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
    Opens key:
    Opens key:
                                                                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}
    Opens key:
                                                                HKCU\software\classes\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\progid
    Opens key:
                                                                HKCR\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}\progid
    Opens key:
                                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
    Opens key:
                                                                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_xmlhttp
                                                                HKLM\software\wow6432node\microsoft\internet explorer\abouturls
    Opens key:
    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
                                                                HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_block_lmz_img
                                                                HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_block_lmz_img
                                                                HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{317d06e8-5f24-433d-bdf7-bdf7-bdf\} = \{317d06e8-5f24-433d-bdf7-bdf\} = \{317d06e8-5f24-433d-bdf\} = \{3
   Opens key:
79ce68d8abc2}
    Opens key:
                                                                HKCR\activatableclasses\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
    Opens key:
                                                                HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}
                                                                HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
    Opens kev:
    Opens key:
                                                                HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\treatas
                                                                HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
    Opens key:
                                                                HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{317d06e8-5f24-433d-bdf7-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-1434b-143
    Opens key:
79ce68d8abc2}\inprocserver32
                                                                HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
   Opens kev:
79ce68d8abc2}\inprocserver32
                                                                HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{317d06e8-5f24-433d-bdf7-14434\} \\ node \mid clsid \setminus \{317d06e8-5f24-433d-bdf7-14434\} \\ node \mid clsid \mid clsid \mid \{317d06e8-5f24-433d-bdf7-14434\} \\ node \mid clsid \mid 
    Opens key:
79ce68d8abc2}\inprochandler32
                                                                HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
    Opens key:
79ce68d8abc2}\inprochandler32
   Opens key:
                                                                HKCU\software\classes\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler
                                                                HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
    Opens key:
79ce68d8abc2}\inprochandler
                                                                HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
    Opens key:
c6b61110b681}\instance
    Opens key:
                                                                HKCR\wow6432node\clsid\fae3d380-fea4-4623-8c75-c6b61110b681\\instance
                                                                HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
    Opens key:
c6b61110b681}\instance\disabled
                                                                HKCR\wow6432node\clsid\{fae3d380-fea4-4623-8c75-
    Opens kev:
c6b61110b681}\instance\disabled
                                                                HKCU\software\classes\wow6432node\clsid\{7ed96837-96f0-4812-b211-
    Opens key:
f13c24117ed3}\instance
                                                                HKCR \setminus wow 6432 node \\ clsid \\ \{7ed 96837 - 96f0 - 4812 - b211 - f13c24117ed3\} \\ \\ instance
    Opens key:
    Opens key:
                                                                HKLM\software\wow6432node\microsoft\avalon.graphics
    Opens key:
                                                                HKCU\software\microsoft\avalon.graphics
    Opens key:
                                                                HKCU\software\classes\wow6432node\clsid\{7835eae8-bf14-49d1-93ce-
533a407b2248}\instance
    Opens key:
                                                                HKCR\wow6432node\clsid\{7835eae8-bf14-49d1-93ce-533a407b2248}\instance
    Opens key:
                                                                HKLM\software\microsoft\windowsruntime\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}
                                                                HKCR\activatableclasses\clsid\{72b624df-ae11-4948-a65c-351eb0829419}
    Opens kev:
```

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{72b624df-ae11-4948-a65c-ae11-4948-ae11-$

Opens key:

```
351eb0829419}
                                                                                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-351eb0829419}
      Opens key:
      Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\treatas
      Opens kev:
                                                                                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-351eb0829419}\treatas
      Opens key:
                                                                                         HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{72b624df-ae11-4948-a65c-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-4948-ae11-
351eb0829419}\inprocserver32
                                                                                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-
      Opens key:
351eb0829419}\inprocserver32
      Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\inprochandler32
      Opens key:
                                                                                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\inprochandler32
     Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\inprochandler
      Opens key:
                                                                                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\inprochandler
      Opens key:
                                                                                         HKLM\software\microsoft\windowsruntime\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}
                                                                                         HKCR\activatableclasses\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
      Opens key:
      Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}
                                                                                         HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
      Opens kev:
      Opens key:
                                                                                         HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{88d96a05 - f192 - 11d4 - a65f - f192 
0040963251e5}\treatas
                                                                                         HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
      Opens key:
      Opens key:
                                                                                         HKCU\software\classes\wow6432node\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32
                                                                                         HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-
      Opens key:
 0040963251e5}\inprocserver32
                                                                                         HKCU\software\classes\wow6432node\clsid\{88d96a05-f192-11d4-a65f-
     Opens kev:
```

0040963251e5}\inprochandler32

HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-Opens key:

0040963251e5}\inprochandler32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{88d96a05 - f192 - 11d4 - a65f - f192 - f192$ Opens key:

0040963251e5}\inprochandler

HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-Opens kev:

0040963251e5}\inprochandler

HKLM\software\wow6432node\microsoft\msxml60 Opens key:

HKCU\software\classes\wow6432node\clsid\{05af94d8-7174-4cd2-be4a-Opens key:

4124b80ee4b8}\instance

HKCR\wow6432node\clsid\{05af94d8-7174-4cd2-be4a-4124b80ee4b8}\instance Opens key: HKCU\software\classes\wow6432node\clsid\{01b90d9a-8209-47f7-9c52-Opens kev:

e1244bf50ced}

HKCR\wow6432node\clsid\{01b90d9a-8209-47f7-9c52-e1244bf50ced} Opens kev: HKCU\software\classes\wow6432node\clsid\{01b90d9a-8209-47f7-9c52-Opens key:

e1244bf50ced}\containers

Opens key: HKCR\wow6432node\clsid\{01b90d9a-8209-47f7-9c52-e1244bf50ced}\containers

HKCU\software\classes\wow6432node\clsid\{e7e79a30-4f2c-4fab-8d00-Opens key:

394f2d6bbebe}

HKCR\wow6432node\clsid\{e7e79a30-4f2c-4fab-8d00-394f2d6bbebe} Opens key: HKCU\software\classes\wow6432node\clsid\{e7e79a30-4f2c-4fab-8d00-Opens key:

394f2d6bbebe}\containers

 $HKCR\wow6432 node\clsid\{e7e79a30-4f2c-4fab-8d00-394f2d6bbebe}\containers$ Opens key:

HKCU\software\classes\wow6432node\clsid\{7f12e753-fc71-43d7-a51d-Opens key:

92f35977abb5}

HKCR\wow6432node\clsid\{7f12e753-fc71-43d7-a51d-92f35977abb5} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{7f12e753-fc71-43d7-a51d-

92f35977abb5}\containers

Opens key: $\label{locality} HKCR\wow6432 node\clsid\{7f12e753-fc71-43d7-a51d-92f35977abb5}\containers$ Opens key: HKCU\software\classes\wow6432node\clsid\{43324b33-a78f-480f-9111-

9638aaccc832} HKCR\wow6432node\clsid\{43324b33-a78f-480f-9111-9638aaccc832} Opens key: HKCU\software\classes\wow6432node\clsid\{43324b33-a78f-480f-9111-Opens kev:

9638aaccc832}\containers

HKCR\wow6432node\clsid\{43324b33-a78f-480f-9111-9638aaccc832}\containers Opens kev:

Opens key: HKCU\software\classes\wow6432node\clsid\{dde33513-774e-4bcd-ae79-

02f4adfe62fc}

Opens key: $HKCR\wow6432 node\clsid\{dde33513-774e-4bcd-ae79-02f4adfe62fc}$ HKCU\software\classes\wow6432node\clsid\{dde33513-774e-4bcd-ae79-Opens kev:

02f4adfe62fc}\containers

Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{aa7e3c50-864c-4604-bc04-

8b0b76e637f6} Opens key: HKCR\wow6432node\clsid\{aa7e3c50-864c-4604-bc04-8b0b76e637f6} Opens kev: HKCU\software\classes\wow6432node\clsid\{aa7e3c50-864c-4604-bc04-

8b0b76e637f6}\containers

Opens kev:

Opens key: HKCU\software\classes\wow6432node\clsid\{72b624df-ae11-4948-a65c-

351eb0829419}\containers

Opens key: HKCU\software\classes\wow6432node\clsid\{9f66347c-60c4-4c4d-ab58-Opens kev:

d2358685f607}

HKCR\wow6432node\clsid\{9f66347c-60c4-4c4d-ab58-d2358685f607} Opens key: HKCU\software\classes\wow6432node\clsid\{9f66347c-60c4-4c4d-ab58-Opens key:

d2358685f607}\containers

HKCR\wow6432node\clsid\{9f66347c-60c4-4c4d-ab58-d2358685f607}\containers Opens key:

Opens kev: HKCU\software\classes\wow6432node\clsid\{50b1904b-f28f-4574-93f4-

0bade82c69e9} HKCR\wow6432node\clsid\{50b1904b-f28f-4574-93f4-0bade82c69e9} Opens kev: HKCU\software\classes\wow6432node\clsid\{50b1904b-f28f-4574-93f4-Opens key:

Obade82c69e9}\containers

HKCR\wow6432node\clsid\{50b1904b-f28f-4574-93f4-0bade82c69e9}\containers Opens key:

Opens kev: HKCU\software\classes\wow6432node\clsid\{356f2f88-05a6-4728-b9a4-

1bfbce04d838}

Opens key: HKCR\wow6432node\clsid\{356f2f88-05a6-4728-b9a4-1bfbce04d838} Opens key:

1bfbce04d838}\containers

HKCR\wow6432node\clsid\{356f2f88-05a6-4728-b9a4-1bfbce04d838}\containers Opens key: Oueries value: HKLM\svstem\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Oueries value:

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

Queries value:

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

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

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

us[alternatecodepage]

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

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

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

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

HKCU\software\microsoft\windows Queries value:

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\mbox{\sc microsoft\windows} & nt\current\sc version\sc mage file execution \end{tabular}$ Oueries value:

options\dllnxoptions[usefilter]

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

options\dllnxoptions[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKLM\software\microsoft\windows Queries value:

nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[83497c45d30bcb551f5f55f3f63b6fa1] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]

HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]

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

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

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]

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

Queries value: HKLM\system\currentcontrolset\control\wmi\security[5c8bb950-959e-4309-

8908-67961a1205d5]

HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[createuricachesize]

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

settings[createuricachesize]

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

settings[createuricachesize]

Queries value:

settings[createuricachesize] HKLM\software\policies\microsoft\windows\currentversion\internet

Oueries value: settings[enablepunycode]

Queries value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

settings[enablepunycode]

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

```
settings[enablepunycode]
                                   HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[security_hklm_only]
                                   HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main[frametabwindow]
  Oueries value:
                                   HKCU\software\microsoft\internet explorer\main[framemerging]
                                   HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
  Oueries value:
  Oueries value:
                                   HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main[sessionmerging]
  Queries value:
                                   HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Oueries value:
                                   HKLM\software\wow6432node\microsoft\internet
explorer\main[admintabprocs]
  Queries value:
                                   HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  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]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Queries value:
08002b30309d}\shellfolder[attributes]
  Queries value:
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[restrictedattributes]
  Oueries value:
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[foldervalueflags]
                                   HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
  Queries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}1
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[]
  Oueries value:
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                                   HKCU\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff1
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
  Oueries value:
  Queries value:
                                   HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
                                  HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[threadingmodel]
                                  HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                   HKLM\system\setup[oobeinprogress]
  Queries value:
  Queries value:
                                   HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                   HKLM\software\microsoft\rpc[idletimerwindow]
                                   \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Queries value:
settings[svncmode5]
                                   HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:
HKLM \label{lem:hklm} White the software \label{lklm} White the 
33be-4251-ba85-6007caedcf9d}[category]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[name]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[parentfolder]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[description]
  Oueries value:
33be-4251-ba85-6007caedcf9d}[relativepath]
  Oueries value:
```

```
33be-4251-ba85-6007caedcf9d}[parsingname]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[infotip]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[localizedname]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[icon]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[security]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresource]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
 Queries value:
33be-4251-ba85-6007caedcf9d}[localredirectonly]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[roamable]
 Queries value:
33be-4251-ba85-6007caedcf9d}[precreate]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[stream]
 Queries value:
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[attributes]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[foldertypeid]
 Oueries value:
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
 Queries value:
                  HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[cache]
 Queries value:
                  HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
 Queries value:
                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders[cache]
                  HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsapiforcrack]
                  HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature http username password disable[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
                  HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
 Oueries value:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                  HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_handling[*]
                  HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                  HKCU\software\microsoft\windows\currentversion\internet
 Queries 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:
                  HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
 Queries value:
                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[disablekeepalive]
                  HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[idnenabled]
 Queries value:
                  \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[preconnectlimit]
```

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

Queries value:

```
settings[preresolvelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sqmhttpstreamrandomuploadpoolsize]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
 Queries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[proxyhttp1.1]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
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
 Oueries value:
settings[disablebasicoverclearchannel]
                          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[utf8servernameres]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings[connecttimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
```

```
Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                         settings\5.0\cache[scavengecachefilelimit]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                         Queries value:
settings[dialupuselansettings]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                         Queries value:
settings[bypasssslnocachecheck]
 Oueries value:
                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
                         Queries value:
settings[nocheckautodialoverride]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonzonecrossing]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[alwaysdrainonredirect]
 Queries value:
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[warnonhttpstohttpredirect]
 Queries value:
                         HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[tcpautotuning]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000002 \ [packed catalog item]
 Queries value:
```

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Queries 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\00000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 000000000001 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000003 [library path] \\ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Queries value:
- HKLM\system\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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000004 [enabled]$

Oueries value:

HKLM\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:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000004 [provider info]$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace _catalog5 \ catalog_entries \ 00000000005 [library path]$ Oueries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 0000000000005[providerid]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 0000000000005 \ [address family]$ Queries value:

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

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

Queries 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\00000000005[providerinfo] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace _ catalog 5 \ catalog _ entries \ 000000000006 [library path]$ Queries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 0000000000006[providerid]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily]

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

Oueries value:

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000006 [provider in fo]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

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

settings[proxysettingsperuser]

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

settings[badproxyexpirestime]

HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enableautodial]

Oueries value:

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

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

settings[globaluseroffline]

Oueries value:

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

settings[disablebranchcache]

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

settings[usefirstavailable]

HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[combinefalsestartdata]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[disablefalsestartblacklist]

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

settings[enforcep3pvaliditv]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value:

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

HKCR\protocols\handler\res[clsid] Oueries value:

Oueries value: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[]

Queries value: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[inprocserver32]

Queries value: $HKCR \land wow 6432 node \land clsid \land \{3050f3bc-98b5-11cf-bb82-11cf-bb8$

00aa00bdce0b}\inprocserver32[] HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-Oueries value: 00aa00bdce0b}\inprocserver32[threadingmodel] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_legacy_dispparams[83497c45d30bcb551f5f55f3f63b6fa1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[*] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_object_caching[83497c45d30bcb551f5f55f3f63b6fa1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_object_caching[*] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_document_compatible_mode[*] Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay] HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-Oueries value: 91a2-7b624e0e7244] Queries value: HKLM\system\currentcontrolset\control\wmi\security[7f8e35ca-68e8-41b9-86fe-d6adc5b327e7] HKLM\software\wow6432node\microsoft\internet explorer\application Queries value: compatibility[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKCU\software\microsoft\internet explorer\domstorage[totallimit] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit] Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_browser_emulation[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_browser_emulation[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding] HKLM\software\policies\microsoft\internet Queries value: explorer\security[disablesecuritysettingscheck] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\4[flags] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKLM\system\currentcontrolset\control\session Oueries value: manager[safeprocesssearchmode] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[specialfolderscachesize] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[specialfolderscachesize] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize] $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ Queries value: settings[specialfolderscachesize] Oueries value: c0e9-4171-908e-08a611b84ff6}[category] Oueries value: c0e9-4171-908e-08a611b84ff6}[name] Queries value: c0e9-4171-908e-08a611b84ff6}[parentfolder] Queries value: c0e9-4171-908e-08a611b84ff6}[description] Queries value: $HKLM \label{lem:hklm} Which was the simulation of the second of the se$ c0e9-4171-908e-08a611b84ff6}[relativepath] Queries value:

 $HKLM \label{lem:hklm} Which was the simulation of the second of the se$

c0e9-4171-908e-08a611b84ff6}[infotip] Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ flocal redirect only \ label{eq:figure}$

Queries value

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value

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

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]

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

settings[urlencoding]

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

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

 $explorer\\ \texttt{main}\\ \texttt{feature}_restrict_res_to_lmz[83497c45d30bcb551f5f55f3f63b6fa1.exe]$

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

explorer\main\featurecontrol\feature_restrict_res_to_lmz[*]

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

explorer\main\featurecontrol\feature_mime_sniffing[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

explorer\main\featurecontrol\feature_mime_sniffing[*]

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

settings[istextplainhonored]

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

explorer\main\featurecontrol\feature_feeds[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

explorer\main\featurecontrol\feature_feeds[*]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-24 cf-9 d55-7 b8 e7 f15 7091 \ficon \fill \fi$

Queries value:

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

Oueries value:

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

Oueries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifthed fib32785-6fba-4fcf-9d55-7b8e7f157091\fifthed fixed fib2785-7b8e7f157091\fifthed fixed fib2785-7b8e7f157091\fifthed fixed fixe$

Oueries value:

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

Queries value

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

Oueries value

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

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

Queries value: folders[local appdata]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite 10e22-4760-9 afe-ea 3317b 67173 \cite 20e3 for the local part of the local part of$

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{area} Hklm \end{area} Hklm \end{area} The constant \end{area} Hklm \end{area} The constant \end{area} Hklm \end{area} The constant \end{area} The cons$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In construction \end{array} The substruction \en$

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value: $HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]$

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

settings\5.0\cache\content[cachelimit]

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Oueries value:

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

Queries value:

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

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[cachelimit]

Oueries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

Oueries value:

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

Queries value

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

Queries value

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

Queries value

 $\label{thm:local-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(d9dc8a3b-b784-432e-a781-5a1130a75963)\cite{Local-redirectonly}\cite{Local-redirec$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[publishexpandedpath] Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[attributes]
Oueries value:

Queries value.

 $\label{thm:microsoftwindows} HKLM software \wow 6432 node \windows \current version \explorer \folder descriptions \def d9dc 8a3b-b784-432e-a781-5a1130a75963 \folder type id \end{substitute}$

Queries value:

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

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

folders[history]

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

settings\5.0\cache\history[cachelimit]

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[local appdata]

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

settings[proxyenable]

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

reporting\wmr[disable]

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

 $explorer\\ \texttt{main}\\ \texttt{feature}_protocol_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]$

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

explorer\main\featurecontrol\feature_protocol_lockdown[*]

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

settings\zones\0[2703]

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

settings\zones\0[2703]

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

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

00aa00686f13}\inprocserver32[inprocserver32]

```
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Queries value:
00aa00686f13}\inprocserver32[]
 Oueries value:
                          HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
                          HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrollinset]
 Queries value:
                          HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
 Oueries value:
                          HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zonemap[ieharden]
 Queries value:
                          HKCU\software\microsoft\internet explorer\flipahead[notificationdelay]
                          HKCR\protocols\handler\about[clsid]
 Oueries value:
 Queries value:
                          HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]
 Queries value:
                          HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
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]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[2106]
                          HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
 Queries value:
 Queries value:
                          HKCU\software\microsoft\internet
explorer\main[minimumsystemtimerresolution]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main[minimumsystemtimerresolution]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[renderingloopmaxtime]
                          HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Queries value:
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
 Queries value:
                          HKCU\software\microsoft\internet explorer[rtfconverterflags]
                          HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[anchor underline]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[css_compat]
                          \label{lem:hkcu} \verb+KKCU\+ software \verb+\microsoft\+ internet explorer \verb+\main[expand alt text]+ \\
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[display inline images]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[display inline videos]
 Oueries value:
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet explorer\main[display
inline videos]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[play_background_sounds]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[play_animations]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[print_background]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main[print_background]
                          HKCU\software\microsoft\internet explorer\main[smoothscroll]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[xmlhttp]
 Oueries value:
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[show image placeholders]
                          HKCU\software\microsoft\internet explorer\main[disable script debugger]
 Queries value:
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[disable diagnostics mode]
                          HKLM\software\wow6432node\microsoft\internet explorer\main[disable
 Oueries value:
diagnostics model
                          HKCU\software\microsoft\internet explorer\main[move system caret]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[usehr]
                          HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[q300829]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\main[cleanup htcs]
 Queries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[xdomainrequest]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main[xdomainrequest]
 Queries value:
                          HKCU\software\microsoft\internet explorer\main[domstorage]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\main[jscriptprofilecacheeventdelay]
                          HKCU\software\microsoft\internet
 Oueries value:
explorer\international[default_codepage]
                          HKCU\software\microsoft\internet explorer\international[autodetect]
 Oueries value:
 Oueries value:
                          HKCU\software\microsoft\internet
explorer\international\scripts[default_iefontsizeprivate]
 Queries value:
                          HKCU\software\microsoft\internet explorer\settings[anchor color]
                          HKCU\software\microsoft\internet explorer\settings[anchor color visited]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\internet explorer\settings[anchor color hover]
```

Queries value: Queries value: size1

Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font

HKCU\software\microsoft\internet explorer\settings[always use my colors]

HKCU\software\microsoft\internet explorer\settings[always use my font

face]

Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited

hyperlinks]

Oueries value: HKCU\software\microsoft\internet explorer\settings[use anchor hover

color1

HKCU\software\microsoft\internet explorer\settings[miscflags] Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\policies[allow

programmatic cut_copy_paste]

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

settings[disablecachingofsslpages]

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

settings[disablecachingofsslpages]

HKCU\software\microsoft\internet explorer\pagesetup[print_background] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefontsize]

Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsizeprivate] HKCU\software\microsoft\internet Oueries value: explorer\international\scripts\3[iepropfontname]

Queries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefixedfontname]

Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]

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

explorer\main\featurecontrol\feature_restrict_filedownload[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

explorer\main\featurecontrol\feature_restrict_filedownload[*]

 $HKCR \land e569bde7-a8dc-47f3-893f-fd2b31b3eefd \\ []$ Queries value:

Queries value: $HKCR\wow6432 node\clsid\{e569bde7-a8dc-47f3-893f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f3-895f-a8dc-47f-a8dc-47f-a8dc-47f-a8dc-47f-48dc-47f-a8dc-47f-48dc-47f-a8dc-47f$ fd2b31b3eefd}\inprocserver32[inprocserver32]

Queries value:

HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893ffd2b31b3eefd}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserver32[threadingmodel]

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

vector[vml]

HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie] Oueries value:

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

explorer\main\featurecontrol\feature_zone_elevation[83497c45d30bcb551f5f55f3f63b6fa1.exe]

HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_zone_elevation[*]

HKCR\mime\database\content type\text/xml[clsid] Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\0[2700]

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

settings\zones\0[2700]

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

explorer\main\featurecontrol\feature_xssfilter[83497c45d30bcb551f5f55f3f63b6fa1.exe]

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

explorer\main\featurecontrol\feature_xssfilter[*]

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

settings\zones[securitysafe]

HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner] Oueries value:

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

rights[protectedmodeoffforallzones]

HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel] Queries value:

Oueries value: HKLM\software\microsoft\olefdefaultaccesspermission1

Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic$ provider[type]

Queries value:

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

provider[image path]

Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Queries value:

HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]

HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] Oueries value:

Queries value: HKLM\software\microsoft\cryptography[machineguid] HKCR\wow6432node\interface\{00000134-0000-0000-c000-Oueries value:

00000000046}\proxystubclsid32[]

HKLM\software\microsoft\rpc\extensions[ndroleextdll] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\0[icon]

Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0[minlevel]

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

settings\zones\0[recommendedlevell

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

settings\zones\0[currentlevel]

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

settings\zones\1[icon]

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

settings\zones\1[minlevel]

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

```
settings\zones\1[recommendedlevel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\1[currentlevel]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[2500]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\1[2500]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\2[icon]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[minlevel]
 Queries value:
                           HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\zones\2[recommendedlevel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\2[currentlevel]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[2500]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\2[2500]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[icon]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[minlevel]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[recommendedlevel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[currentlevel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[2500]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[2500]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\4[icon]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\4[minlevel]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\4[recommendedlevel]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[currentlevel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\4[2500]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\4[2500]
                           HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
 Queries value:
                           HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mshtml_autoload_ieframe[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zones\0[1400]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\0[2106]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[2106]
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[cointernetcombineiuricachesize]
 Oueries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[cointernetcombineiuricachesize]
                           HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_shim_mshelp_combine[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                           HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
 Queries value:
explorer\main\featurecontrol\feature_shim_mshelp_combine[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\connections[defaultconnectionsettings]
 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[migrateproxy]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyoverride]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[autodetect]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\connections[savedlegacysettings]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
 Queries value:
                           HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
```

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns secure name query fall back]$ HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [direct access query order]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [queryipm atching]$ HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register primary name]$ Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value:

 $\label{lem:hklmsystem} HKLM \ system \ current controls et \ services \ dns cache \ parameters [registration maxaddress count] \\ Queries \ value:$

```
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
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]
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts enderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
                          HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
 Queries value:
HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[winhttplowercasehost]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history[daystokeep]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[2700]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\3[2700]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[]
 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\user agent[compatible]
 Queries value:
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings\5.0\user agent[compatible]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[version]
 Queries value:
                          HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\5.0\user agent[version]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\user agent[platform]
                                                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\user agent[platform]
    Queries value:
                                                          HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]
                                                          HKLM\software\wow6432node\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[83497c45d30bcb551f5f55f3f63b6fa1.exe]
    Oueries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
    Oueries value:
                                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver[83497c45d30bcb551f5f55f3f63b6fa1.exe]
    Oueries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
    Oueries value:
                                                         HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
    Oueries value:
HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\peerdist\service[enable]
    Oueries value:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
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\software\wow6432node\microsoft\windows\currentversion\internet
   Oueries value:
settings[securityidiuricachesize]
                                                          HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\zones\3[1a10]
                                                         HKCU\software\microsoft\internet explorer\main[operationaldata]
    Oueries value:
                                                          HKCU\software\microsoft\internet
    Queries value:
explorer\browseremulation[cvlistxmlversionlow]
    Oueries value:
                                                         HKCU\software\microsoft\internet
explorer\browseremulation[cvlistxmlversionhigh]
                                                          HKCU\software\microsoft\internet
    Queries value:
explorer\browseremulation[iecompatversionlow]
                                                          HKCU\software\microsoft\internet
    Queries value:
explorer\browseremulation[iecompatversionhigh]
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
    Queries value:
settings[warnonintranet]
    Queries value:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ in the lemma + the lemma 
    Queries value:
settings[warnonintranet]
    Queries value:
                                                          settings[warnonintranet]
                                                          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
    Oueries value:
    Queries value:
                                                          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
    Queries value:
    Oueries value:
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                                          HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Queries value:
f4ceaaf59cfc}\inprocserver32[]
                                                         HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Oueries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
    Queries value:
                                                         HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
                                                          HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
    Queries value:
                                                          HKLM\software\wow6432node\microsoft\direct3d\drivers[size]
    Oueries value:
    Oueries value:
                                                          HKLM\software\wow6432node\microsoft\direct3d\drivers[name]
    Oueries value:
HKLM\software\wow6432node\microsoft\direct3d\dx6textureenuminclusionlist[size]
    Oueries value:
HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus direct3d \setminus dx6texture enuminclusion list[name]
    Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8
55779daa70e9}[searchlist]
    Oueries value:
806e6f6e6963}[enabledhcp]
    Oueries value:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-8
55779daa70e9}[registrationenabled]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
    Oueries value:
```

55779daa70e9}[domain]

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}\[dhcpv6domain1\]

Oueries value:

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

Oueries value:

Oueries value:

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

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \time faces \end{497e1de57-d6fa-11e1-be62-806e6f6e6963} \ [registration enabled]$

Oueries value:

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

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} [domain]$

Queries value:

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

Oueries value:

Queries value:

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

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

Queries value:

Queries value:

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

Queries value:

Oueries value

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

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

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

Queries value:

Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]Queries value:HKCU\software\microsoft\internet explorer\gpu[adapterinfo]Queries value:HKCU\software\microsoft\internet explorer\recovery[autorecover]Queries value:HKCU\software\microsoft\windows\currentversion\internet

settings\zones\0[2000]

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

settings\zones\0[2000]

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

discovery[sound]

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

```
Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1400]
 Queries value:
                          HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1608]
 Oueries value:
                          HKCU\appevents\schemes[]
 Oueries value:
                          HKCU\appevents\schemes\apps\explorer\navigating\.current[]
 Oueries value:
                          HKCU\appevents\schemes\apps\explorer\navigating\.current[default flags]
 Oueries value:
                          HKLM\system\currentcontrolset\control\nls\codepage[28591]
 Oueries value:
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings\zones\3[{a8a88c49-5eb2-4990-a1a2-0876022c854f}]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_subdownload_lockdown[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
                         HKCU\appevents\schemes\apps\explorer\activatingdocument\.current[]
 Queries value:
 Queries value:
                          HKCU\appevents\schemes\apps\explorer\activatingdocument\.current[default
flags]
                          HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
 Oueries value:
 Queries value:
                          HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_script[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                          HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_block_lmz_script[*]
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-0ff4dc41e755}[]
 Oueries value:
 Queries value:
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-
0ff4dc41e755}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-
 Queries value:
Off4dc41e755}\inprocserver32[]
 Queries value:
                         HKCR\wow6432node\clsid\{16d51579-a30b-4c8b-a276-
Off4dc41e755}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[57277741-3638-4a4b-
bdba-0ac6e45da56c]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1201]
                          HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-8bc445b9828f}[]
 Queries value:
 Queries value:
                         HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
8bc445b9828f}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
 Oueries value:
8bc445b9828f}\inprocserver32[]
                         HKCR\wow6432node\clsid\{842a1268-6e6a-465c-868f-
 Oueries value:
8bc445b9828f}\inprocserver32[threadingmodel]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_use_windowedselectcontrol[83497c45d30bcb551f5f55f3f63b6fa1.exe]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_use_windowedselectcontrol[*]
                         HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-00aa00bdce0b}[]
 Oueries value:
 Oueries value:
                         HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
 Queries value:
00aa00bdce0b}\inprocserver32[1
 Queries value:
                         HKCR\wow6432node\clsid\{3050f391-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet explorer\abouturls[blank]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_about_protocol_ie7[*]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_block_lmz_img[83497c45d30bcb551f5f55f3f63b6fa1.exe]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}[]
 Queries value:
 Queries value:
                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
 Oueries value:
79ce68d8abc2}\inprocserver32[]
                         HKCR\wow6432node\clsid\{317d06e8-5f24-433d-bdf7-
 Oueries value:
79ce68d8abc2}\inprocserver32[threadingmodel]
 Queries value:
                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-351eb0829419}[]
 Queries value:
                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-
351eb0829419}\inprocserver32[]
                         HKCR\wow6432node\clsid\{72b624df-ae11-4948-a65c-
 Oueries value:
351eb0829419}\inprocserver32[threadingmodel]
 Queries value:
                         HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
                         HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-
 Oueries value:
```

0040963251e5}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-

0040963251e5}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{88d96a05-f192-11d4-a65f-

0040963251e5}\inprocserver32[threadingmodel]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\history[cacheprefix]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]